SHORTCOMINGS IN INFORMATION SHARING FACILITATES TRANSNATIONAL ORGANIZED CRIME

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Homeland Security Studies

by

DANIEL J. TUCKER, MAJOR, U.S. ARMY
B.S., Excelsior College, Albany, New York, 2009

Fort Leavenworth, Kansas
2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
9-06-2017	Master's Thesis	AUG 2016 – JUN 2017

4. TITLE AND SUBTITLE

Shortcomings in Information Sharing Facilitates Transnational Organized Crime

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Daniel J. Tucker, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study asks what shortcoming exists hindering information sharing across the U.S. Government to combat transnational organized crime (TOC). A comprehensive review of national strategies, law, and scholarly works establish the immediate security and economic threat posed by criminal organizations worldwide. The confluent business models shared by terrorist and TOC organizations requires an equally unified effort to combat these threats. By employing a levels of analysis approach to disaggregate national level, organizational level and individual level factors, four gaps emerge to combat TOC. First, divergent strategies to combat terrorist and TOC organizations are revealed. Second, the current process for information sharing relies on gate keepers access to stove piped information. Third, the absence of a lead agency to combat TOC. Finally, bureaucratic boundaries to sharing information persist. To address these shortcomings, five recommendations are provided. First, a single national strategy clearly representing the convergence between terrorist and TOC organizations. Second, the Director of National Intelligence must have the authorities necessary to unify the intelligence community (IC). Third, reorganization of the IC is urgently needed. Fourth, designate the National Counter Terrorism Center as the lead agency to combat TOC. Finally, a directive to migrate all government networks to cloud technology.

15. SUBJECT TERMS

Information Sharing, Transnational Organized Crime, Terrorist Organizations, Terrorism Prevention, Cloud Computing, Organizational Culture, NCTC, Intelligence Community, DNI

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	89	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Daniel J. Tucker

Thesis Title: Shortcomings in Information Sharing Facilitates Transnational Organized Crime

Approved by:

_____, Thesis Committee Chair
Michael H. McMurphy, MMAS

_____, Member
O. Shawn Cupp, Ph.D.

_____, Member
MAJ Joseph L. Strawn, LL.M

Accepted this 10th day of June 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SHORTCOMINGS IN INFORMATION SHARING FACILITATES TRANSNATIONAL ORGANIZED CRIME, by MAJ Daniel J. Tucker, 89 pages.

This study asks what shortcoming exists hindering information sharing across the U.S. Government to combat transnational organized crime (TOC). A comprehensive review of national strategies, law, and scholarly works establish the immediate security and economic threat posed by criminal organizations worldwide. The confluent business models shared by terrorist and TOC organizations requires an equally unified effort to combat these threats.

By employing a levels of analysis approach to disaggregate national level, organizational level and individual level factors, four gaps emerge to combat TOC. First, divergent strategies to combat terrorist and TOC organizations are revealed. Second, the current process for information sharing relies on gate keepers access to stove piped information. Third, the absence of a lead agency to combat TOC. Finally, bureaucratic boundaries to sharing information persist.

To address these shortcomings, five recommendations are provided. First, a single national strategy clearly representing the convergence between terrorist and TOC organizations. Second, the Director of National Intelligence must have the authorities necessary to unify the intelligence community (IC). Third, reorganization of the IC is urgently needed. Fourth, designate the National Counter Terrorism Center as the lead agency to combat TOC. Finally, a directive to migrate all government networks to cloud technology.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my wife Jessica, and our children, Courtney, Chris, Kelsey and Hope, for all of their love and support through this process. Their sacrifice and patience was instrumental in my success in both the Command and General Staff College and this study.

I was particularly fortunate to have Mr. Michael McMurphy as my chair. His leadership and expertise is second to none. Additionally, Dr. Shawn Cupp and MAJ Joseph Strawn ensured intellectual rigor and helped me through many difficulties. This committee dedicated countless hours the successful completion of this thesis.

Special thanks go out to my instructors: LTC (Dr.) Jerry Moon, Dr. Harry Laver, Dr. Sean Kalic, Mr. Matt Broaddus, and Mr. Robert Martin. In my twenty-four years of service I have never met a more intelligent, dedicated and talented group of professionals.

TABLE OF CONTENTS

Page

ACRONYMS

CIO	Chief Information Officer
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
IBM	Interactive Behavior Model
IC	Intelligence Community
IT	Information Technology
NCTC	National Counter Terrorism Center
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
NSS	National Security Strategy
OMB	Office of Management and Budget
PM-ISE	Program Manager, Information Sharing Environment
TOC	Transnational Organized Crime
UNODC	United Nations Office on Drugs and Crime

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

Overview

> Despite a long and successful history of dismantling criminal organizations and developing common international standards for cooperation against transnational organized crime, not all of our capabilities have kept pace with the expansion of 21st century transnational criminal threats.
>
> — President Barack Obama,
> *Strategy to Combat Transnational Organized Crime*

The purpose of this research is to examine the shortcomings in efforts to combat transnational organized crime (TOC) organizations. The United States and the international community label violent extremist organizations as "terrorist" organizations. This label restricts possible efforts, and potentially the range of options, to target organizations, which have yet to carry out violence. It must be understood that whether organizations conduct violent acts or seek monetary gain through illicit endeavors, both are criminal organizations. Terrorist organizations resource violence through criminal activities. Efforts must be broadened to combat terrorist acts through further study of all TOC syndicate's effects on less developed countries. Criminal activities provide the means for violent extremist organizations to control and oppress these populations. Despite efforts through national strategies and legislation directing and encouraging information sharing, processes and execution gaps persist. Approaches to addressing these shortcomings must not be constrained to establishment of new organizations or requirements for additional resources. A thorough analysis of current government organizations charters, authorities, and resourcing is required.

The 2015 *National Security Strategy* (NSS) identifies TOC as a strategic priority.[1] Illicit activities of these criminal organizations include drug trafficking, human trafficking, smuggling of migrants, trading of firearms, trafficking in natural resources, illegal trade of wildlife, sale of fraudulent medicines, and cybercrime.[2] The Office on Drugs and Crime (UNODC) estimates money laundering alone accounted for between 2 and 5 percent of the global gross domestic product in 2015, at least $1.6 trillion in 2009.[3] By targeting these criminal organizations through a whole of government approach, working closely with multinational law enforcement and partner nation support, degradation of violent extremist organizations is feasible.[4] Understanding the confluence of TOC and terrorist organizations is paramount to unifying global partners to defeating this threat.[5]

In reaction to the tragedies the United States endured on September 11, 2001, a congressional commission investigated how such events were able to take place and how

---

[1] U.S. President, *National Security Strategy* (Washington, DC: The White House, 2015).

[2] United Nations Office on Drugs and Crime (UNODC), *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes* (Vienna: United Nations, 2011), accessed November 13, 2016, https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

[3] Ibid., 5.

[4] Tamara Makarenko, "The Crime–Terror Continuum: Tracing the Interplay between Transnational Organized Crime and Terrorism," *Global Crime* 6, no. 1 (February 2004): 129-145.

[5] Chris Dishman, "The Leaderless Nexus: When Crime and Terror Converge," *Studies in Conflict and Terrorism* 28 (2005): 237-252.

to prevent future attacks.[6] These findings recommended the creation of the Department of Homeland Security (DHS), Office of the Director of National Security, and the National Counter Terrorism Center (NCTC).[7] The establishment of these organizations were efforts to unify previously isolated departments and agencies across the federal government.

The 9/11 Commission investigation uncovered information sharing procedures were either nonexistent or not followed.[8] This commission also identified the numerous "stove piped" computer networks.[9] These networks created barriers between agencies within the government to share information horizontally.[10] Presently, though numerous accomplishments are made daily, information systems continue to lack the horizontal interconnectivity to seamlessly share information. This persistent lack in real time information sharing presents gaps for criminals and terrorist to exploit.

Federal government department and agencies operate in these independently operated information systems with strictly controlled access. Though computer technology has evolved exponentially since the turn of the 21st century, the U.S.

---

[6] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: Government Printing Office, 2004).

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid.

Government is resistant to employ technologies such as cloud technology.[11] Cloud computing was recognized for interoperability and cost savings resulting in the "Cloud First Policy" issued in 2011 directed by the Obama administration.[12] Even though every administration creates policies and strategies to address federal government computer system heterogeneity, lack of legislation enables the construction of information silos.

Primary Research Question

What shortcoming exists hindering information sharing across the U.S. Government to combat TOC?

Secondary Research Questions

What is the link between terrorism and TOC?

How is information currently shared across the federal government?

What current technology exists to enable information sharing?

Assumptions

The primary assumption in this study is criminal organizations will continue to exploit knowledge gaps and lack in unity of effort to meet their nefarious goals. These organizations pose an immediate threat to U.S. national security and economic interests. The United States and the international community were mobilized by the terrorist attacks on September 11, 2001. In the wake of these events information, sharing gaps

[11] Frank Konkel, "Moving to the Cloud? Change Your Culture First," Nextgov, April 13, 2016, accessed January 25, 2017, http://www.nextgov.com/cloud-computing/2016/04/moving-cloud-change-your-culture-first/127453.

[12] Vivek Kundra, *Federal Cloud Computing Strategy* (Washington, DC: The White House, 2012).

were revealed. A criminal organization must not be allowed to inflict such an event before shortcomings in information sharing are identified and addressed.

Numerous organizational and technological measures were enacted following the terrorist attacks on 9/11. The unprecedented reorganization of the U.S. Government and policy is ongoing. By examining the confluence between terrorism and TOC, the U.S. Government can apply the lessons learned from counter terrorism efforts to close information gaps to combat TOC.

Technology can close gaps in information sharing to combat TOC with appropriate resourcing, cybersecurity, and access control. The innovation in cloud computing within the private sector has revolutionized business practices. Cloud computing technology provides the ability break down boundaries and operationalize national information against adversaries. The inability to share information in real time nationally and internationally hinders the ability to prevent future domestic and international violent extremism.

Definitions

Cloud Computing: A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. , networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[13]

[13] Kundra.

Crime: An illegal act for which someone can be punished by the government.[14]

Information: The communication or reception of knowledge or intelligence.[15]

Information Gap: A deficiency or disparity in access to information.[16]

Information Sharing: The fact of different departments, companies, etc. using the same information.[17]

Information Technology (IT): The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.[18]

Intelligence: The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.[19]

---

[14] Merriam-Webster, "Crime," accessed June 5, 2017, https://www.merriam-webster.com/dictionary/crime.

[15] Merriam-Webster, "Information," accessed June 5, 2017, https://www.merriam-webster.com/dictionary/information.

[16] Oxford Dictionary, "Information Gap," accessed June 5, 2017, https://en.oxforddictionaries.com/definition/information_gap.

[17] Cambridge Dictionary, "Information Sharing," accessed June 5, 2017, http://dictionary.cambridge.org/us/dictionary/english/information-sharing.

[18] Merriam-Webster, "Information Technology," accessed June 5, 2017, https://www.merriam-webster.com/dictionary/information%20technology.

[19] Joint Chiefs of Staff, Joint Publication 2, *Joint Intelligence* (Washington, DC: Government Printing Office, 2013).

Interagency: Of or pertaining to U.S. Government agencies and departments.[20]

Terrorism: the unlawful use or threat of violence especially against the state or the public as a politically motivated means of attack or coercion.[21]

Transnational Organized Crime (TOC): self-perpetuating associations of individuals who operate, wholly or in part, by illegal means and irrespective of geography.[22]

Limitations

The study of national efforts to identify shortcomings constrains this research to a qualitative approach. Qualitative analysis of strategies, policies, law, and technology is required to reveal shortcomings and potential solutions. Quantitative approaches for further study may be warranted to offer precision on gaps revealed in this study.

TOC has existed for thousands of years. The shortcomings in information sharing within the U.S. Government also has a long history. This study is limited to national efforts undertaken following the terrorist attacks on September 11, 2001 to present.

Delimitations

This study is limited to U.S. strategies, policies, law, and regulations coupled with scholarly work researching terrorism, TOC and cloud computing. Given the vast amount

---

[20] Joint Chiefs of Staff, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, November 8, 2010, as amended through January 31, 2011).

[21] Merriam-Webster, "Terrorism," accessed June 5, 2017, https://www.merriam-webster.com/dictionary/terrorism.

[22] Federal Bureau of Investigation, "Transnational Organized Crime," accessed January 25, 2017, https://www.fbi.gov/investigate/organized-crime.

of previous research on individual criminal and terrorist organizations, case studies show little explanatory power. This thorough analysis of national measures seeks to identify strategic, organizational, and individual shortcomings in combatting TOC. Only unclassified information will be used.

The researcher's education is drawn from the Irregular Warfare Scholars Program at the U.S. Army Command and General Staff College. This program includes study in political science, sociology, psychology, economics, and special operations doctrine. Experience is derived from observations of U.S. Government strategic initiatives to combat TOC while assigned to the Joint Improvised Threat Defeat Organization. This organization works closely with interagency partners to defeat terrorist organizations and identify criminal organizations supporting terrorist.

Significance of the Study

This research will identify the shortcomings in information sharing to combat TOC. In order to clearly define the current gaps in information sharing, this research will disaggregate strategy, organizational considerations, and individual psychologic factors. This approach allows for an understanding of shortcomings in sharing information from the national level to performance. A detailed historical review of actions taken by the U.S. Government following the terrorist attacks on 9/11 to the present will be studied. To clearly identify gaps in information sharing to combat TOC, subsequent research questions must be answered.

The linkages between terrorist organizations and TOC organizations will be researched in an effort to aggregate the threat to U.S. national security and economic interests. To have a premise to build upon, a detailed study of current processes to share

information across the government is conducted. This research will also include technological innovations incorporated by the private sector and the federal government to explore the viability of potential solutions.

Chapter 2 is the study of national policies, laws, scholarly articles, journals, and books. This chapter is framed into three sections corresponding to the secondary research questions. Chapter 3 will outline the methodology used in the research. Chapter 4 will delineate the findings of qualitative research conducted to articulate gaps in the U.S. Government's current processes to share information to combat TOC. Chapter 5 will include a conclusion of this study and present recommendations to improve information sharing.

CHAPTER 2

LITERATURE REVIEW

The intent of this literature review is to frame the research process to identify shortcomings in information sharing across the U.S. Government to combat TOC. An evolution in methods led to a whole of government approach to combat terrorism, but limited methodologies are implemented to combat TOC. Current practices of targeting organizations based on violent acts is inherently reactionary. The goal must be to interdict violence through pursuing resourcing. A deeper understanding of criminal threats is needed for national security and economic prosperity.

This chapter is organized into three sections corresponding to the secondary research questions. This approach allows for precision in answering secondary research questions. The first section, "Terrorism and Transnational Organized Crime," will study the link between terrorism and TOC. Confluence between these organizations will establish the national security threat posed by TOC organizations.

The second section, "Information Sharing Post 9/11," examines how information sharing changed following the attacks on 9/11. This section will establish a baseline to understand current information sharing procedures. The third section, "Evolution of Technology," explores the federal government recognition of immerging technology and advances in technology within the private sector. The evolution of IT in the 1990s revolutionized U.S. Government business practices forever.

Scholarly research is limited to the era following the fall of the Soviet Union. This is intentional to scope the research with the emergence of information technology.

Additionally, the evolution in the character of criminal activities in the global economy provides contemporary context to the threat imposed.

Transnational Organized Crime and Terrorism

TOC is as old as governments and international trade.[23] In the wake of the post-Cold War world the scope and scale of TOC has exponentially increased due to the lack of state sponsorship of terrorist activities by the Soviet Union and their allies.[24] The convergence of these terrorist organizations and TOC organizations emerged in the wake of globalization and the international community's ability to regulate it.[25]

There is no consensus on a clear definition of TOC among practitioners or theoreticians due to the complex criminal activities conducted in an organized manner.[26] In an effort to provide precision as to the criminal activities that are termed as TOC the Federal Bureau of Investigation describes these organizations as:

> groups are self-perpetuating associations of individuals who operate, wholly or in part, by illegal means and irrespective of geography. They constantly seek to obtain power, influence, and monetary gains. There is no single structure under which TOC groups function—they vary from hierarchies to clans, networks, and cells, and may evolve into other structures. These groups are typically insular and protect their activities through corruption, violence, international commerce,

---

[23] Michael Woodiwiss, "Transnational Organized Crime: The Global Reach of American Concept," in *Transnational Organized Crime: Perspectives on Global Security*, eds. Peter Gill and Adam Edwards (New York: Routledge, Taylor and Francis Group, 2004), 50-75.

[24] Thomas M. Sanderson, "Transnational Terror and Organized Crime: Blurring the Lines," *SAIS Review* 24, no. 1 (2004): 49-61.

[25] UNODC, *The Globalization Of Crime A Transnational Organized Crime Threat Assessment*.

[26] Ibid.

> complex communication mechanisms, and an organizational structure exploiting national boundaries.[27]

This characterization of the activities provides context to the complexity in which these organizations operate. Examples of these activities include child pornography, human trafficking, drug trafficking, firearms trafficking, migrant smuggling, environmental resource trafficking, maritime piracy, cybercrime, and product counterfeiting.[28] These international crimes evolve as markets develop for goods or service.[29]

Criminal markets dramatically transformed following the collapse of the Soviet Union.[30] The rise in conflicts was resourced by transnational criminal organizations, growing in business acumen to capitalize on revenue.[31] The former Soviet Union conducted or supported worldwide campaigns consisting of proxy wars, "national liberation" movements, and terrorist acts from the onset of the Cold War.[32] Violent organizations rapidly adapted to this loss of state sponsorship to further their greed or

---

[27] Federal Bureau of Investigation, "Transnational Organized Crime," accessed June 5, 2017, https://www.fbi.gov/investigate/organized-crime.

[28] UNODC, *The Globalization Of Crime A Transnational Organized Crime Threat Assessment*.

[29] Ibid.

[30] Phil Williams and Dimitri Vlassisi, "Combating Transnational Crime: Concepts, Activities and Responses," *Transnational Organized Crime* 4, no. 3/4 (1998): 1-384.

[31] Ibid.

[32] Ray S. Cline and Yonah Alexander, *Terrorism - The Soviet Connection* (Bristol, PA: Crane, Russak and Co., 1984).

grievance.[33] These criminal organizations overlap with terrorist organizations where they can only be distinguished by motive. Criminal organizations seek financial gain and terrorist organizations seek political, sometimes religious goals. [34] Since the 1990s, these organizations generated power and wealth across the globe without an international effort to fight this growing threat, until 9/11.[35]

Emerging in the wake of the horrible events perpetrated on 9/11, the linkage between terrorism and TOC emerges. These costly events spawned a wave of counter terrorism measures initiated by the United States and allies. The effects from the terrorist attacks changed the world.

In the wake of 9/11, the United States declared a Global War on Terrorism uniting allies to defeat global terrorism. The Patriot Act of 2001 addressed the requirement to interdict terrorist organizations' ability to finance activities by including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.[36] In describing the threat, this law stated, "money laundering, estimated by the International Monetary Fund to amount to between 2 and 5 percent of global gross domestic product, which is at

---

[33] Harvey W. Kushner, *Terrorism in America: A Structured Approach to Understanding the Terrorist Threat* (Springfield, IL: Charles C. Thomas, 1998).

[34] John R. Wagley, *Transnational Organized Crime: Principal Threats and U.S. Responses* (Washington, DC: Library of Congress, 2006).

[35] Sanderson.

[36] U.S. Congress, *USA Patriot Act*, Public Law 107-56 (Washington, DC: Government Printing Office, October 26, 2001).

least $600 billion annually.[37] Increasing substantially since 2002, estimates grew be in excess of two trillion dollars as of 2016.[38]

In addition to these escalating figures in money laundering, criminal trafficking is estimated to be in excess of $870 billion dollars as of 2009.[39] In 2011, the Obama administration released a strategy to combat TOC. This strategy reveals a whole of government approach in an effort to combat TOC.[40] This strategy contains five key objectives:

> 1. Protect Americans and our partners from the harm, violence, and exploitation of transnational criminal networks.
>
> 2. Help partner countries strengthen governance and transparency, break the corruptive power of transnational criminal networks, and sever state-crime alliances.
>
> 3. Break the economic power of transnational criminal networks and protect strategic markets and the U.S. financial system from TOC penetration and abuse.
>
> 4. Defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.

---

[37] U.S. Congress, *USA Patriot Act*, section 302.

[38] United Nations Office on Drugs and Crime, "Money Laundering and Globalization," United Nations, accessed January 25, 2017, https://www.unodc.org/unodc/en/money-laundering/globalization.html.

[39] United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes* (Vienna, Austria: United Nations, 2011). 7.

[40] U.S. President, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington, DC: The White House, July 2011).

5. Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime.[41]

This comprehensive strategy outlines the requirements for increased intelligence capability and information sharing both domestically and internationally.[42] As Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, William Wechsler, remarked at The Washington Institute on April 26, 2012, "success depends on driving our government toward operating like a network so that we are as flexible and agile in our actions as our adversaries are in theirs."[43]

As in any organization, survival is based on resiliency.[44] The ability for criminal organizations to adapt quickly is attributed to the structure or architecture of their networks.[45] These networks are loosely linked with highly clustered, redundant hubs, which are more resistant to random attacks.[46] An effort to explain how criminal networks are constructed and persevere, the actor-network theory treats objects as part of social

---

[41] U.S. President, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington, DC: The White House, July 2011), 1

[42] Ibid.

[43] William F. Wechsler, "Combating Transnational Organized Crime" (Remarks Prepared for Delivery at the Washington Institute, Washington, DC, August 26, 2012), accessed June 5, 2017, http://www.washingtoninstitute.org/html/pdf/WechslerPrepared20120426.pdf.

[44] Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law, Crime and Justice* 37 (2009): 182-196.

[45] Ibid.

[46] Ibid.

networks.[47] This approach is powerful to explain how illicit goods or modes of distribution are intertwined in a complex social organization interconnected within an ever globalizing world. Targeting goods or distribution platforms should not be disaggregated during efforts taken to combat terrorism or TOC.

Evolving in the wake of U.S. and international efforts following 9/11, terrorist organizations created internal criminal capabilities to fund operations.[48] This transformation can be attributed to the observation that criminal organizations will not cooperate with terrorist organizations to advance aims and interests.[49] Legacy criminal organizations mirrored corporate structures to sustain programs and improve operational capabilities.[50] More modern studies have revealed that U.S. and international efforts broke down many of these hierarchical structures causing a "leaderless nexus" to emerge.[51] This phenomenon of large flattened organizational structures with little control over their extensive network allows for desperate low to mid-level criminals and terrorist groups to converge to attain their malevolent ends.[52] The leaders of these terrorist enterprises provide little more than inspiration to its members with increasingly less

---

[47] John Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity," *Systems Practice and Action Research* (1992): 379-393.

[48] Sanderson.

[49] Chris Dishman, "Terrorism, Crime, and Transformation," *Studies in Conflict and Terrorism* 24, no. 1 (2001): 43-58.

[50] Sanderson.

[51] Dishman, "The Leaderless Nexus: When Crime and Terror Converge."

[52] Ibid.

control over actions conducted in the organization's name.[53] Additionally allowing leadership to claim credit or refute involvement in these activities. The relationship of these two groups is graphically depicted below.

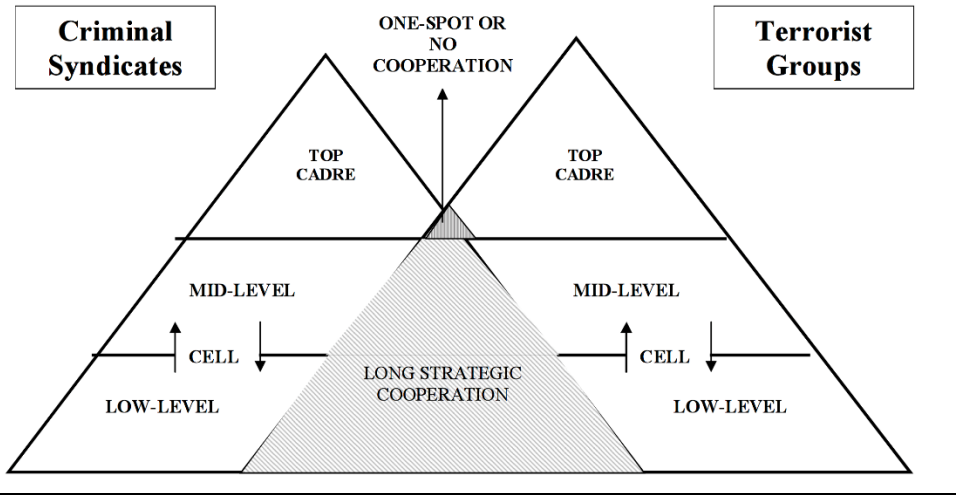

Figure 1. Nexus of Criminal Syndicates and Terrorist Groups

Source: Chris Dishman, "The Leaderless Nexus: When Crime and Terror Converge," *Studies in Conflict and Terrorism* 28 (2005): 245.

As figure 1 shows, the collaboration between criminal and terrorist organizations have critical implications for U.S. security.[54] These hybrid organizations pose unique challenges to law enforcement and intelligence.[55] Criminal investigations, domestic

[53] Dishman, "The Leaderless Nexus: When Crime and Terror Converge."

[54] Ibid.

[55] Ibid.

intelligence, and foreign intelligence efforts overlap.[56] Separating these organizations cause a gap in knowledge between departments, agencies and partners.[57]

The prevailing theme emerging is the confluence between TOC and terrorist organizations. Though organized crime and terrorism has existed for centuries, the proliferation of illicit activities following the fall of the Soviet Union is well known. Efforts to combat these threats consistently label them as criminal or terrorist by federal agencies. These labels isolate government actions to holistically address these criminal organizations. Understanding the coordination between TOC and terrorism is vital to national security and economic prosperity.

Information Sharing Post 9/11

In the wake of terrorist attacks conducted on 9/11, the U.S. Government has taken many strides to encourage sharing information across the whole of government. First of these efforts was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.[58] Referred to as the Patriot Act, which this law revised numerous statues, including Titles 8, 12, 15, 18, 20, 31, 42, 49 and 50 of the U.S. Code.[59] Enhancing surveillance capabilities, border security, improving intelligence, and broader authorities to investigate domestic terrorism authorities were modified to combat terrorist threats. Recognized in this act was the gap

[56] Dishman, "The Leaderless Nexus: When Crime and Terror Converge."

[57] Ibid.

[58] U.S. Congress, *USA Patriot Act*.

[59] Ibid.

between federal, state, and local law enforcement agencies and prosecutors.[60] This authorized the Attorney General $50,000,000 to establish regional computer forensics laboratories and provide support to existing laboratories to facilitate and promote information sharing.[61] This initial measure brought to light the need for law enforcement activities to coordinate investigations from the national level to the local level and vice versa.

Following the Patriot Act was the Homeland Security Act of 2002. The DHS integrated all or part of twenty-two federal departments or agencies into a single organization to protect the American homeland.[62] According to Raphael Perl, "The creation of the new department constitutes the most substantial reorganization of the federal government agencies since the National Security Act of 1947, which placed the different military departments under a secretary of defense and created the National Security Council (NSC) and Central Intelligence Agency (CIA)."[63] The creation of the DHS was triggered by the tragic events of 9/11, although the need to converge desperate functions within the government was identified in the 1990s following the United Nations

[60] U.S. Congress, *USA Patriot Act*.

[61] Ibid., section 816.

[62] Department of Homeland Security, "Creation of the Department of Homeland Security," September 24, 2015, accessed January 25, 2017, https://www.dhs.gov/creation-department-homeland-security.

[63] Raphael Perl, "The Department of Homeland Security: Background and Challenges," in *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings, by Committee on Counterterrorism Challenges for Russia and the United States* (Washington, DC: Library of Congress, 2004), 176-184.

bombing in 1993.[64] One of the primary missions of this newly created DHS is "monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking." In 2005, the Secretary of DHS developed a six point plan with one of these being "Enhance information sharing with our partners" which remains unchanged to date.[65] In 2007, the Office of Intelligence and Analysis was established "as a member of the U.S. Intelligence Community (IC) and is the only IC element statutorily charged with delivering intelligence to our state, local, tribal, territorial and private sector partners, and developing intelligence from those partners for the Department and the IC."[66] This effort was to address the requirement to fuse and share national intelligence with local law enforcement to combat terrorism.

Released on July 22, 2004, the 9/11 Commission Report was requested by President George W. Bush and congress to investigate events leading up to the 9/11 terrorist attacks and provide recommendations to prevent further such acts.[67] The report cited in the preface "We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that has been built in a different era to confront dangers.[68] Identifying the shortcomings in information sharing across the

---

[64] Perl, 176-184.

[65] Department of Homeland Security, "Department Six-Point Agenda," September 23, 2013, accessed January 25, 2017, https://www.dhs.gov/department-six-point-agenda.

[66] Department of Homeland Security, "Office of Intelligence and Analysis," accessed January 25, 2017, https://www.dhs.gov/office-intelligence-and-analysis.

[67] National Commission on Terrorist Attacks Upon the United States.

[68] Ibid.

departments and agencies down to the local level the report recommended, "information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."[69] The committee went further to recommend the same quality standards whether in Pakistan or in Texas. Additionally, finding the need to update outdated mainframes that operate on a hub-and-spoke concept to develop the capability to share information horizontally.[70] This task was recommended to be taken up by the newly designated Director of National Intelligence.

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Director of National Intelligence (DNI) to serve as the head of the U.S. IC.[71] This legislation was recommended by the 9/11 Commission following the investigation revealing shortcomings identified within the IC.[72] The commission went on to identify six problems within the IC before and after 9/11: structural barriers to performing joint intelligence work, lack of common standards and practices across the foreign-domestic divide, divided management of national intelligence capabilities, weak capacity to set priorities and move resources, and too many jobs.[73] The DNI is responsible for managing national intelligence priorities, budget, structure, training, and reporting under the

[69] National Commission on Terrorist Attacks Upon the United States.

[70] Ibid.

[71] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004* (Washington, DC: Government Printing Office, 2004).

[72] National Commission on Terrorist Attacks Upon the United States.

[73] Ibid.

president.[74] Additionally, the DNI is the principal authority to manage information sharing across the IC and tasked to establish common information systems, develop enterprise architecture, and include multi-level security protocols and integration capabilities.[75] In an effort to achieve interoperability within the IC, the *Intelligence Community Information Technology Enterprise Strategy 2016-2020* sets three strategic goals: enhance intelligence integration, optimize information assurance to secure and safeguard the IC enterprise, and operate as an efficient, effective IC enterprise.[76] This strategy, initially developed in 2012, is helping agencies share data by utilizing a common virtual desktop with an App Mall for users to download apps and share data on the IC cloud.[77] This technological leap forward will allow the IC to collaborate in real time.[78] Bureaucratic resistance has slowed progress on the Intelligence Community Information Technology Enterprise with former acting Defense Intelligence Agency Director David Shedd stating in March 2015 it would be "easily five years" before fully

[74] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004*.

[75] Ibid.

[76] Office of the Director of National Intelligence, *Intelligence Community Information Technology Enterprise Strategy 2016-2020* (Washington, DC: Government Printing Office, 2016).

[77] Karen J. Bannan, "The Intelligence Community Is Sharing More Data, and Making It More Secure," FedTech, July 22, 2016, accessed January 25, 2017, http://www.fedtechmagazine.com/article/2016/07/intelligence-community-sharing-more-data-and-making-it-more-secure.

[78] Ibid.

implemented.[79] This strategy recognizes the need to fuse intelligence across the IC, only to be hindered by bureaucratic boundaries.

Eventually aligning under the DNI, Congress directed the establishment of Office of the Program Manager, Information Sharing Environment (PM-ISE) in 2004 to share terrorist information across the whole of government.[80] The PM-ISE "has government-wide authority granted by the Congress to serve as a trusted broker facilitating the development of a network-centric ISE by promoting standards and architecture, security and access, and associated privacy protections."[81] Prior to 9/11, law enforcement investigations were conducted at the field office level, which held little regard for national priorities.[82] Expanding the scope of PM-ISE, congress passed the Implementing Recommendations of the 9/11 Commission Act of 2007, adding homeland security and weapons of mass destruction systems integration which expanded the responsibilities of the office from solely terrorist activities.[83] The PM-ISE is responsible for large measures to improve access to national intelligence at regional fusion centers located throughout

[79] Sean Lyngaas, "ICITE Faces Cultural Resistance," *FCW*, March 3, 2015, accessed January 25, 2017, https://fcw.com/articles/2015/03/03/icite-faces-resistances.aspx.

[80] U.S. Congress, *Intelligence Reform and Terrorism Prevention Act of 2004*.

[81] Information Sharing Environment, "The Role of PM-ISE," accessed January 25, 2017, https://www.ise.gov/about-ise/what-ise.

[82] National Commission on Terrorist Attacks Upon the United States.

[83] U.S. Congress, *Implementing Recommendations of the 9/11 Commission Act of 2007* (Washington, DC: Government Printing Office, 2007).

the United States comprised of federal, state, local, and tribal officials.[84] These fusion centers have varying capacity due to dependence on staffing by national agencies to provide system access.[85] This persistent "stove piping" of information is caused by institutional resistance to sharing information due to ego, information is power, coupled with technical and logistic problems.[86] Though these fusion centers mainly focus on terrorism, many have broadened their scope to criminal activities after recognizing the relationship between criminal activities and terrorism.[87]

The prevailing theme emerging is the recognition that information sharing is required to combat threats to national security. To date, efforts to improve information sharing through technology is limited to organizational efforts. The lack of a unified federal government approach to horizontally sharing information persists. Approaches to improve information sharing are the formation of fusion centers at the national and state level.

[84] David L. Carter and Jeremy G. Carter, "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement," *Criminal Justice and Behavior* 36, no. 12 (2009): 1323-1339.

[85] Ibid.

[86] Ibid.

[87] Ibid.

Evolution of Technology

Modern communication networks and internet access provide increased speed, knowledge sharing, collaboration and reduced cost around the world.[88] This is no more evident than in the development of E-Government in the 1990s to streamline and improve efficiency across the institutions within the U.S. Government.[89] This effort to capitalize on the emergence of IT was initiated by the Clinton administration under the National Performance Review launched on March 3, 1993.[90] This initiative was aimed at increasing customer service and streamlining government services, while also reducing the federal workforce by 250,000 jobs.[91] During this period of technological growth, a proliferation of discretely managed systems emerged.[92]

In 2002, congress passed the E-Government Act of 2002, which established a Federal Chief Information Officer under the Office of Management and Budget (OMB).[93] This codified into law the requirement to provide transparency and efficiency across the governments Information Technology (IT) infrastructure.[94] The Bush administration

---

[88] Mohamed Mirghani, Michael Stankoski, and Arthur Murray, "Knowledge Management and Information Technology: Can They Work in Perfect Harmony?" *Journal of Knowledge Management* 10, no. 3 (2006): 103-116.

[89] Jane E. Fountain, "Bureaucratic reform and e-government in the United States: An Institutional Perspective," *Routledge Handbook of Internet Politics* (2009): 99-113.

[90] Ibid.

[91] Ibid.

[92] Ibid.

[93] U.S. Congress, E-Government Act of 2002 (Washington, DC: Government Printing Office, 2002).

[94] Ibid.

identified twenty-four initiatives divided into four portfolios: Government to Citizen, Government to Business, Government to Government, and Internal Efficiency and Effectiveness.[95] E-Authentication is a separate initiative to address security across the twenty-four identified initiatives.[96] In the year prior, the Bush administration initiated an effort named Quicksilver to find "quick wins" in consolidating these networks.[97] This effort was poorly funded due to the federal funding processes where committees within congress appropriate department and agency funding directly making cross-agency projects difficult.[98] The E-Government initiative aimed for citizens to receive high quality service from the government, while reducing the cost to deliver services.[99]

In 2004, President Bush launched the Lines of Business initiative to consolidate and streamline the federal government information systems.[100] The initiative identified five initial lines of business including human resource management, financial management, grants management, federal health architecture, case management and information systems security, adding Information Technology Security Task Force and budget formulation and execution in 2005.[101] This initiative enabled the "lead agency"

---

[95] Fountain.

[96] Ibid.

[97] Ibid.

[98] Ibid.

[99] U.S. President, *The President's Management Agenda* (Washington, DC: The White House, 2002).

[100] Fountain.

[101] Ibid.

approach to networks, where agencies would agree to transfer funding for IT service.[102] Congress increasingly demanded the ability for these funds to be transferred after Memorandums of Understanding were signed.[103] These efforts sought to capitalize on emerging technologies and gain efficiencies.

The concept of cloud computing dates back to 1961, where a utility-based business model of computing power and specific applications might be sold by time sharing techniques.[104] With the lack of capability, the concept waned until emerging technology revitalized cloud computing as a functional reality.[105] The resulting globalization of computing assets shrank the world increasing and adding capacity while not investing in infrastructure.[106] The ability to subscribe or pay-for-use service from a single point of entry for IT services provides IT managers with a more acceptable return on investment.[107]

Cloud computing technology emerged from the dot-com bubble burst in 2001. Amazon developed and implemented a cloud architecture out of this financial crisis.[108] This provided very significant internal efficiencies where in 2002 third-party users were

---

[102] Fountain.

[103] Ibid.

[104] John W. Rittinghouse and James F. Ransome, *Cloud Computing: Implementation, Management, and Security* (Boca Raton, FL: CRC Press, 2009).

[105] Ibid.

[106] Ibid.

[107] Ibid.

[108] Ibid.

allowed access on a utility computing basis.[109] Users were now able to access services and remotely store data in the cloud without having the expertise to manage infrastructure.[110] The revolution that ensued swept the globe.[111]

The U.S. Chief Information Officer, Vivek Kundra, released the *Federal Cloud Computing Strategy* on February 8, 2011.[112] Using the National Institute of Standards and Technology definition of cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[113] This strategy articulates the requirement to improve the efficiency and collaboration within the government to better serve the American public.[114] Articulating the benefits in the table below, a cloud first policy was implemented for all agencies to modify their IT portfolios.

[109] Rittinghouse and Ransome.

[110] Ibid.

[111] Ibid.

[112] Kundra.

[113] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing* (Gaithersburg, MD: National Institute of Standards and Technology, 2011).

[114] Kundra.

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

Figure 2. Cloud Benefits: Efficiency, Agility, Innovation

Source: Vivek Kundra, *Federal Cloud Computing Strategy* (Washington, DC: The White House, 2012), 3.

This measure to capitalize on private sector innovation proposed a $20 billion, of $80 billion, investment in potential spending on cloud computing across the government.[115] This investment is twofold. First, analysis of the 2010 federal budget revealed 30 percent of IT spending was spent on data center infrastructure.[116] Second, investment in the private industry's capacity for government agencies to migrate

[115] Kundra.

[116] Ibid.

services.[117] Following migration to the cloud, subsequent years' budgets will have the ability to increase capacity or reinvest in mission specific requirements.[118]

Federal agencies are presented with a decision framework for migration.[119] This framework is a broad approach that requires a shift in how organizations think about IT.[120] Presented in a three-step process consisting of select, provision, and manage, agencies are provided a planning tool.[121] In selecting which services to move to and when agencies evaluate potential efficiencies along with market availability, security, and current technology lifecycle.[122] Next provisioning requires aggregation of demand where possible, analysis of interoperability and integration, contract effectiveness, and repurposing or decommissioning legacy assets.[123] Finally, managing calls for a shift in mindset from assets to service, training, monitoring of agreements, and vendor re-evaluation to maximize benefits.[124]

Building on all the aforementioned initiatives and strategy, the Federal Chief Information Officer Council (CIOC) released *The Federal Shared Services*

---

[117] Kundra.

[118] Ibid.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Ibid.

Implementation Guide on April 16, 2013. [125] This council is comprised of nineteen CIOs from across the federal government. This document codifies the requirement and provides a guide for agencies to shift to a shared service environment.[126] Introduced is a central Federal Shared Services Catalog for federal agencies to quickly locate and engage commercial shared service providers.[127]

On January 20, 2015, a Congressional Research Service report identified two main drivers of cloud adoption within federal agencies.[128] These drivers were identified at budget concerns and data center consolidation.[129] Budget concerns were a driver in spite of over half of the federal agencies assessing cloud services brought some level of savings.[130] With federal data center closures expected to decrease by 1,100 in 2015, a savings of $3 billion, agencies are forced to shift to cloud computing.[131]

---

[125] Chief Information Officer Council, *Federal Shared Services Implementation Guide* (Washington, DC: Government Printing Office, 2013).

[126] Ibid.

[127] Ibid.

[128] Patricia Moloney-Figliola and Eric A. Fisher, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management* (Washington, DC: Library of Congress, 2015).

[129] Ibid.

[130] Ibid.

[131] Ibid., 22.

Security and management of information systems are the primary concerns with regard to migrating to cloud technology.[132] In an effort to streamline the security assessment and accessibility to cloud vendors, the federal government established the Federal Risk and Authorization Management Program.[133] This program is a result of close collaboration with cybersecurity and cloud experts from agencies across the U.S. Government.[134]

This program uses the approach "do once, use many times" by providing a central repository of vendors that meet federal government requirements. This centralized solution to vendor assessment saves an estimated 30-40 percent of procurement costs.[135] Currently, 102 federal agencies employ cloud computing services through this program.[136]

In spite of these efforts, there are challenges to migrating to cloud services. [137] Many CIOs are concerned with security and not managing and controlling their data centers.[138] This concern is in spite of stated security advantages calling for the need to

---

[132] Kenneth Corbin, "5 Years into the 'Cloud First Policy,' CIOs Still Struggling," *CIO*, April 27, 2016, accessed January 25, 2017, http://www.cio.com/article/3061941/cloud-computing/5-years-into-the-cloud-first-policy-cios-still-struggling.html.

[133] FedRAMP, "FedRAMP Overview," General Services Administration, accessed January 25, 2017, https://www.fedramp.gov/about-us/about/.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Moloney-Figliola and Fisher.

[138] Ibid.

address a culture to trust cloud technology.[139] In a Government Accountability Office report released in September 2014, seven agencies within the U.S. Government were examined on the status of cloud adoption.[140] Findings from this report revealed that these agencies increased eighty services, twenty-one to 101, to the cloud as compared from the 2012 report.[141] The reported savings from the implementation of twenty-two of these services are estimated at $96 million.[142] Another survey was conducted by *Information Week* also in September 2014. This survey of 153 federal government IT executives revealed that 71 percent continued to manage data themselves and 55 percent believed that cloud computing will make data management easier.[143] CIOs understand of the benefits of cloud technology, but lack the will to relinquish perceived control of information.

Benefits from leveraging emerging technology is widely recognized. Administrations enacted policies to integrate computer networks across the federal government for decades. Cloud computing provides organizations the ability to focus less on capability and more on services. Institutional resistance to fully implement this technology due to a perceived lack of trust prevails to this day. This lack of trust, coupled with congressional resourcing processes create opportunities for organizations to operate disparate networks across the federal government.

---

[139] Moloney-Figliola and Fisher.

[140] Ibid.

[141] Ibid., 19.

[142] Ibid., 20.

[143] Ibid.

Other Scholarly Works

In the course of research, numerous masters' theses from the U.S. Army Command and General Staff Officer College, the Naval Postgraduate School, and Senior Service Colleges were studied. In addition, numerous books, journals, articles and government policies and regulations were worthy of inclusion into this thesis.

Summary

Terrorist organizations and TOC organizations are inextricably linked, only separable by desired outcomes. Competing approaches to combat terrorism or TOC, whether foreign or domestic, provide these organizations ability to exploit seams in efforts. By aggregating the threat, policies and laws could address the root causes and capabilities of terrorist organizations. Combatting terrorism through the understanding that TOC is intertwined shows promise to mitigate the ability of violent organizations to build capability to conduct violence. The United States has focused, in large part on combating terrorism through reactive strategies.

Emerging from the tragic events on 9/11 is the recognition that information sharing is essential to combat threats to national security. Existing measures to share information consist primarily of fusion centers, national and local, to share information confined to countering terrorism, homeland security, and weapons of mass destruction. These efforts fail to address the underlying problem of stove piped computer networks. These fusion centers show progress, but to not address cultural barriers between organizations or homogenizing computer networks for rapid dissemination of information.

Over three decades administrations and congress attempted to reduce cost and improve effectiveness of federal computer networks. Cloud technology emerged in the 21st century and is leveraged by private industry, but largely resisted by federal agencies. Enabled by congressional budgeting processes, institutional resistance is due to a perception of loss of control and security concerns. Even after addressing these concerns, organizations continue to resist implementation. This technology provides consumers with the ability to focus resources on service versus management of computer network infrastructure.

During the course of this literature review several areas of concern emerged. These include classified network implications, access control, and cybersecurity. These concerns are outside of the scope of this research, but provide future researchers topics for future study.

CHAPTER 3

RESEARCH METHODOLOGY

Overview

The research design selected for this study is through narrative research. This qualitative analysis on U.S. Government policies, laws, and research is integrated with a robust amount of scholarly works to identify gaps in information sharing to combat TOC. There are four characteristics of qualitative research.[144] The first characteristic of a qualitative research is that the study examines how the individual aspects of the study work together to affect the whole.[145] This study will focus on disaggregate potential barriers to share information to combat TOC to identify shortcomings and recommend potential improvements. Second, in qualitative research the researcher is the primary instrument for data collection and analysis.[146] The author searched, assessed, and fused previous works from a wide array of sources. The third characteristic of qualitative research typically involves fieldwork.[147] Due to time constraints, field work could not be performed and will not be included in this study. The fourth characteristic is that the qualitative research primarily employs an inductive research strategy, built on hypotheses, rather than tests of theory.[148] Due to the scope of diverse research required to

---

[144] Sharan B. Merriam, *Qualitative Research and Case Study Applications in Education* (San Francisco, CA: Jossey-Bass, 1998).

[145] Ibid.

[146] Ibid.

[147] Ibid.

[148] Ibid.

identify shortcomings in information sharing to combat TOC, quantitative research was not suitable for this study.

Data Collection

Due to U.S. national security and international security threats posed by TOC there is an abundant amount of previous research available. Furthermore, cloud technology development and analysis is equally rich in application and research. In an effort to evaluate TOC and cloud technology in concert, all research will be drawn from the actions taken in the wake of the terrorist attacks on 9/11 to date.

This thesis will utilize all available literature on terrorism, TOC, and cloud computing to include U.S. policies, evaluate outcomes, and provide recommendations. An equally considered aspect of this study is the fiscal responsibility of the federal government. This budgetary consideration is to examine future possibilities to unify effort across the whole of government versus establishing organizations as a solution.

Data Analysis

The purpose of this narrative qualitative study is to answer: what shortcoming exists hindering information sharing across the U.S. Government to combat TOC? In order to answer this question, analysis of policy, laws, organizations, and authorities following the tragic events of 9/11 are explored. A detailed investigation of measures enacted and shortfalls will reveal gaps in current policies, law, and approaches to improve information sharing to combat TOC.

The analysis will scrutinize literature in a systematic method through inductive reasoning. This methodology is structured on levels of analysis and will be employed to

examine strategic, organizational, and individual considerations in sharing information.[149] Commonly employed by researchers in international relations, the levels of analysis approach provides the ability to disaggregate complex systems.[150] This methodology offers the ability to analyze the interaction between policy makers, organizations, and decision makers. This framework is designed to accurately identify shortcomings in information sharing from policy to execution.

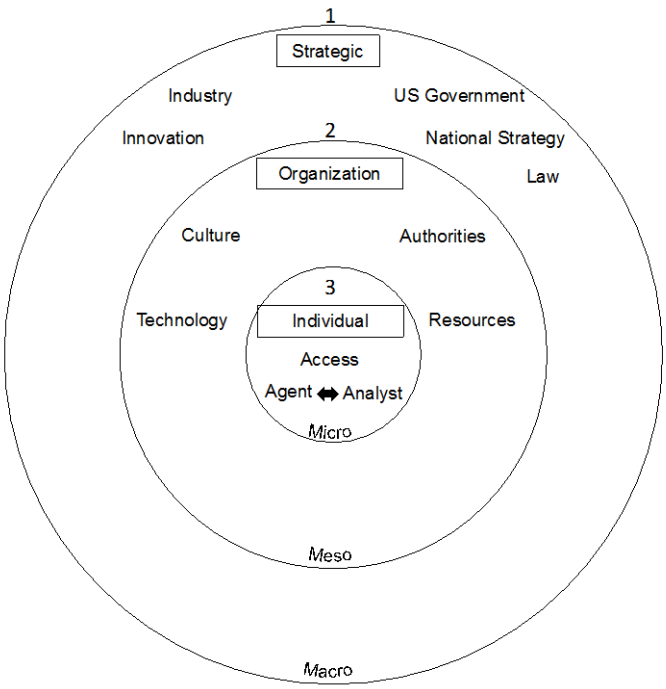

Figure 3. Levels of Analysis

Source: Created by author.

[149] Taku Tamaki, "Levels of Analysis of the International System," in *Encounters with World Affairs: An Introduction to International Relations,* ed. E. Kavalski (Farnham: Ashgate, 2015), 85-106.

[150] Ibid.

First, strategic level of analysis will analyze national strategies and law concerning terrorism, TOC, and information sharing. These documents are examined individually and holistically to isolate in information sharing policies and legislation. Shortcomings identified at this macro level allow for national policy and law recommendations.

Second, organization level investigates organizational cultural aspects to information sharing within federal, state, and local government departments and agencies. For the purposes of this research, individual organizations are not measured. Introduced in this section are the cultural considerations pertaining to information sharing. Further examining the measures enacted to improve information sharing following the terrorist attacks on 9/11. This meso level analysis intends to identify gaps in historic and current measures to share information.

Third, individual level of analysis examines psychological factors to share information.

Introduced at this micro level of analysis is the Interactive Behavioral Model (IBM). This model was developed through integrating the Theory of Reasoned Action, Theory of Planned Behavior, and other theories.[151] This model is best described by Dr. Kasprzyk, stating "IBM was developed through discussions and consensus among major behavioral theorists and has been modified through empirical work."[152] This

[151] Daniel E. Montano and Danuta Kasprzyk, "Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model," in Kasisomayajula Viswanath, and Karen Glantz. *Health Behavior and Health Education. Theory, Research, and Practice*, ed. Barbara K. Rimer (San Fransisco, CA: John Wiley and Sons, 2008), 67-96.

[152] Ibid., 91.

comprehensive model examines various considerations to predict human behavior. Previously employed by researchers studying mental health, transportation preferences, and marketing amongst others this model is widely recognized by scholars for providing explanatory power. This micro level analysis is limited to introducing the psychological factors involved in sharing information.

The IBM identifies five factors that affect behavioral performance.[153] An individual must be motivated to perform a recommended behavior, intention to perform the behavior, without which the behavior is doubtful.[154] This intention is drawn first from the attitude toward the behavior, whether the individual supports or does not support performing the behavior.[155] Second, the perceived norms take the social aspects one feels to carry out, or not, the behavior.[156] Third, personal agency accounts for one's personal functioning and environmental events.[157] All of these factors result in the motivation to carry out a behavior, depicted in figure 4 as intention to perform the behavior.

Once an individual is motivated to follow through with a behavior additional factors are considered. Subsequent factors include knowledge to carry out the behavior, without which intention is mute.[158] Also considered are environmental constraints, which

[153] Montano and Kasprzyk.

[154] Ibid.

[155] Ibid.

[156] Ibid.

[157] Ibid.

[158] Ibid.

need to be mitigated to conduct a desired behavior.[159] Another factor is the salience of the behavior.[160] The final factor is habit, which takes in account the experience performing the behavior.[161] Commonly employed in empirical studies, the IBM is utilized to provide context to individual considerations in information sharing. This model incorporated within the third level of analysis is employed to provide precision in identifying shortcomings in current practices to share information. Below is an illustration of the IBM:

[159] Montano and Kasprzyk.

[160] Ibid.

[161] Ibid.

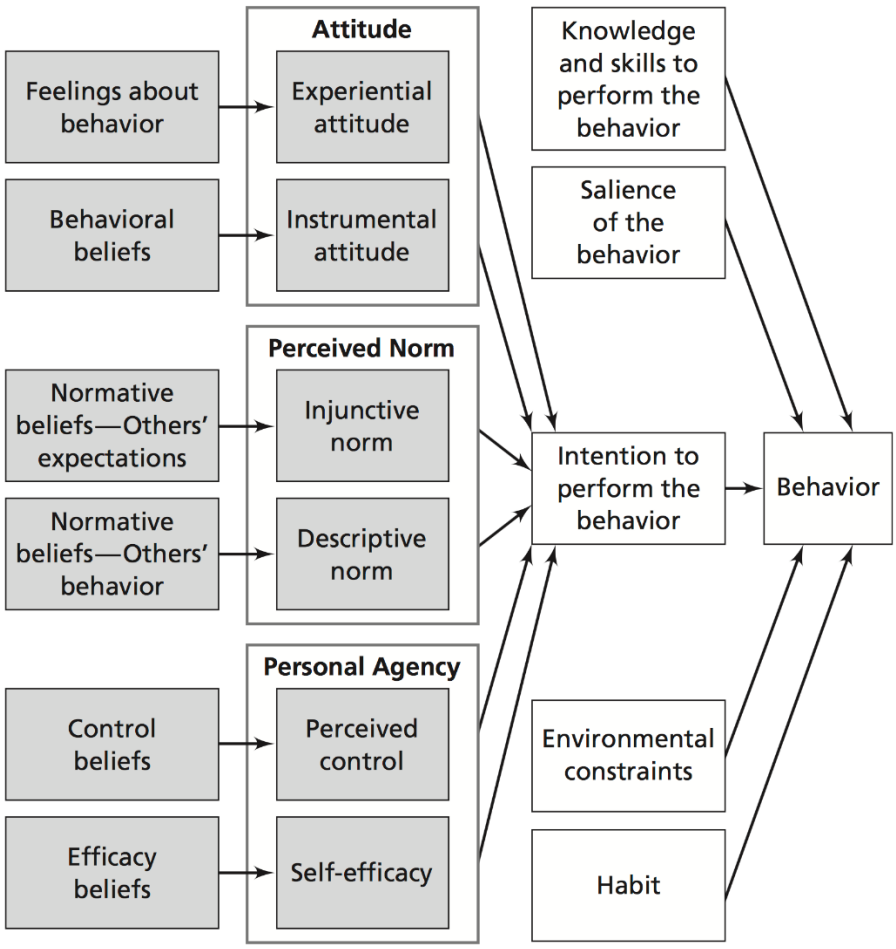

Figure 4. Integrated Behavior Model

Source: Daniel E. Montano and Danuta Kasprzyk, "Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model," in Kasisomayajula Viswanath, and Karen Glantz. *Health Behavior and Health Education. Theory, Research, and Practice*, ed. Barbara K. Rimer (San Fransisco, CA: John Wiley and Sons, 2008), 77.

Possible Sources of Bias

Narrative research presents potential bias due to the dependence on the researcher's ability to analyze information subjectively. The vast and varying amount of literature studied during the course of constructing this thesis provided the necessary

information to complete the qualitative analysis and answer the research questions posed. The author recognizes his personal experiences introduce potential bias. This bias is mitigated through selection of peer reviewed scholarly sources and U.S. Government documents and studies. Additionally, the researcher lacks the professional education and training in the topics examined to bias the analysis and findings.

Summary

This chapter describes the design and methodology employed to organize and analyze this research. A vast amount of literature on terrorism, TOC, and cloud technology is scrutinized to answer the research questions posed. This narrative analysis is conducted through a levels of analysis approach to disaggregate the strategic, organizational and individual level actors. This approach examines the interaction between these levels to identify information sharing gaps from policy to execution. Introduced at the individual level is the Interactive Behavioral Model. This model intends to analyze the risk in current information sharing procedures. Finally, identifying and mitigating bias is addressed.

Chapter 4 details the analysis and reveals the shortcomings in information sharing at the strategic, organizational, and individual levels. This chapter is constructed to answer the secondary research questions posed in this thesis. These findings provide the basis for the conclusion and recommendations in chapter 5.

Chapter 5 is the culmination of this thesis providing the conclusions of the analysis and recommendations to address the information sharing gaps revealed. Included in this chapter are shortcomings identified outside the scope of this research. This chapter

answers the primary and secondary research questions, providing insights for future studies in this area of research.

CHAPTER 4

ANALYSIS

This chapter will answer the primary research question of what shortcoming exists hindering information sharing across the U.S. Government. Preeminent to U.S. national security is the ability to deny adversaries ability to carry out violent acts. Terrorist organizations, just as other violent organizations or states, rely on resources from criminal activities, diasporas, and donor nations. The world is progressively interconnected inside a global economy. This expansion of technology and trade, employed by nefarious entities, provide opportunities to identify and prosecute criminal enterprises in an effort to restrict resources of violent extremists. Not since the attack on Pearl Harbor on December 7, 1941 has the U.S. homeland suffered loss of life and destruction on this scale. Tragically, both events changed the world forever. These attacks caught the United States unprepared. In reaction, the Bush administration and congress acted quickly by passing legislation to prevent further attacks.

The purpose of this chapter is to analyze current shortcomings in U.S. Government efforts to combat TOC. This chapter is organized into three sections corresponding to the levels of analysis introduced in chapter 3. The first section, titled "Strategic Level," analyzes national policies and laws. The linkage between terrorism and TOC at the national level are examined in this section. The gaps revealed in this section are isolated at the national level to provide policy recommendations.

The second section, titled "Organizational Level," examines federal departments' and agencies' cultural and IT aspects to identify shortcomings in information sharing to

combat TOC. These organizations transcend administrations and perform required functions under authorities and resources granted by congress.

The final section, titled "Individual Level," explores psychological factors related to information sharing. This level of analysis employs the Integrated Behavioral Model described in chapter 3. This model is predominately utilized in quantitative analysis, but is a powerful tool to introduce the human dimension currently relied upon to share information. This introduction to human psychology is employed to identify the risk in current practices.

Strategic Level

> The events of September 11, 2001, taught us that weak states, like Afghanistan, could pose as great a danger to our national interests as strong states. Poverty does not make poor people into terrorists and murderers. Yet poverty, weak institutions, and corruption can make weak states vulnerable to terrorist networks and drug cartels within their borders.[162]

Since 1990, the number of rogue states has drastically increased.[163] Terrorist and criminal organizations within these states share attributes such as oppression of populations and squandering national resources to achieve their goals.[164] These organizations disregard international law, sponsor terrorism, and reject basic human rights.[165] The 2002 NSS identifies the need to strengthen U.S. intelligence capabilities

---

[162] U.S. President, *National Security Strategy* (Washington, DC: The White House, 2002).

[163] U.S. President, *The President's Management Agenda* (Washington, DC: The White House, 2002).

[164] Ibid.

[165] U.S. President, *National Security Strategy*, 2002.

both foreign and domestic. Clearly recognizing that law enforcement and intelligence activities must fuse information, five initiatives are identified:

> 1. Strengthening the authority of the Director of Central Intelligence to lead the development and actions of the Nation's foreign intelligence capabilities
>
> 2. Establishing a new framework for intelligence warning that provides seamless and integrated warning across the spectrum of threats facing the nation and our allies
>
> 3. Continuing to develop new methods of collecting information to sustain our intelligence advantage
>
> 4. Investing in future capabilities while working to protect them through a more vigorous effort to prevent the compromise of intelligence capabilities
>
> 5. Collecting intelligence against the terrorist danger across the government with allsource analysis[166]

In the 2006 NSS, the Bush administration emphasizes the institutional reforms implemented in prior years. These measures are discussed further in this chapter under "Organizational Level." Clearly articulated in this strategy is the requirement to increase the capabilities and capacity of federal departments and agencies to conduct counter terrorism activities both at home and abroad. Traditionally domestic institutions have an increasing role in foreign security. This strategy identifies how globalization is exploited by criminals involved in illicit trade. This illicit trade of drugs, humans, or sex undermines governance, rule of law, and security in weak or failing states.

Not until the Obama administration's 2010 NSS was the crime-terror nexus clearly established, stating:

> Transnational criminal threats and illicit trafficking networks continue to expand dramatically in size, scope, and influence—posing significant national security challenges for the United States and our partner countries. These threats cross

[166] U.S. President, *National Security Strategy,* 2002.

> borders and continents and undermine the stability of nations, subverting government institutions through corruption and harming citizens worldwide. Transnational criminal organizations have accumulated unprecedented wealth and power through trafficking and other illicit activities, penetrating legitimate financial systems and destabilizing commercial markets. They extend their reach by forming alliances with government officials and some state security services. The crime-terror nexus is a serious concern as terrorists use criminal networks for logistical support and funding.[167]

For the first time, the threat of cybercrime is linked to existing terrorist and criminal networks. This strategy clearly expresses the economic risk posed by these cybercrimes, costing billions of dollars to the global economy every year. Additionally articulated is the effect of these cybercrimes on financial institution trust across the globe.[168]

This strategy called for the United States to devise and execute a collective strategy to address these criminal enterprises.[169] President Obama identifies the need for a "multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency" to combat transnational criminal networks. The administration also cites the requirement to strengthen domestic security. This strategy calls to facilitate the integration of computer networks across federal, state, and

[167] U.S. President, *National Security Strategy* (Washington, DC: The White House, 2010).

[168] Ibid.

[169] Ibid.

local agencies.[170] This homogenous network would empower intelligence agencies to exchange messages, share information, and collaborate with law enforcement.[171]

Expanding on the 2010 NSS, the Obama administration issued a *Strategy to Combat Transnational Organized Crime* in July 2011. This was the first national strategy focused on TOC. The president stated, "Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing."[172] This strategy is the result of a U.S. Government comprehensive review of international organized crime.[173] Identifying fifty-six priority actions to combat TOC domestically and on international partners, these actions seek to "enhance intelligence and information sharing; protect the financial system and strategic markets against TOC; strengthen interdiction, investigations, and prosecutions; disrupt drug trafficking and its facilitation of other transnational threats; and build international capacity, cooperation, and partnerships."[174]

By expanding on the previous crime-terror nexus, this strategy links insurgency within this threat establishing a crime-terror-insurgency nexus.[175] This strategy recognizes the criminal activities which resource terrorist organizations such as al-

---

[170] U.S. President, *National Security Strategy,* 2010.

[171] Ibid.

[172] U.S. President, *Strategy to Combat Transnational Organized Crime.*

[173] Ibid.

[174] Ibid.

[175] Ibid.

Qa'ida, Hizballah, Revoluntionary Armed Forces of Colombia, and al-Shabaab.[176] These criminal acts include, but are not limited to, drug trafficking, kidnapping for ransom, and extortion to fund terrorist acts.[177] The "facilitators" identified in this strategy link licit-illicit relationships through semi-legitimate actors.[178] These organizations utilize shell companies with off shore banking and front companies to exploit the global marketplace to conduct illegal activities.[179]

Enhanced intelligence support to combat TOC is required.[180] Priority actions within the *National Strategy to Combat Transnational Organized Crime* of 2011 call for updating the National Intelligence Priorities Framework. These classified IC priorities need to align with the TOC threat and require increased support by Office of the Director of National Intelligence.[181] Additionally, this strategy directs a strong relationship between federal, state, local, tribal, and territorial authorities to share information.[182] Information sharing between national intelligence and local police is paramount to defend the homeland from these criminal threats.

This *National Strategy to Combat Transnational Organized Crime* is further reinforced by the 2015 NSS. The Obama administration further emphasizes leveraging

---

[176] U.S. President, *Strategy to Combat Transnational Organized Crime.*

[177] Ibid.

[178] Ibid.

[179] Ibid.

[180] Ibid.

[181] Ibid.

[182] Ibid.

the use of all the instruments of national power to dismantle criminal and terrorist networks.[183] The 2015 NSS again emphasizes the need to strengthen efforts to combat criminal enterprises ability to affect national economic and security interests.[184] The impacts of these powerful criminal organizations prevent the development of weak states institutions ability to care for the needs of their people.[185] Information sharing from national to local levels is critical to combat terrorism both homegrown and foreign.

The 2007 *National Strategy for Information Sharing* recognizes the challenges, which continue to exist following the attacks perpetrated on 9/11. Focusing predominately on combating terrorism, this strategy identifies the TOC threat. This interwoven threat is clearly expressed where President Bush states, "Information sharing must be woven into all aspects of counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events."[186] Further supporting the confluence of TOC and terrorism, this strategy cites multiple domestic criminal investigations revealing links to international terrorist organizations. The administration directs the Program Manager, Information Sharing Environment to establish procedures to securely disseminate information across the federal government and to state and local law enforcement. This strategy fails to address information technology shortcomings across the federal government.

---

[183] U.S. President, *National Security Strategy,* 2015.

[184] Ibid.

[185] Ibid.

[186] Ibid., 3.

In 2012, the Obama administration's National Strategy for Information Sharing and Safeguarding builds upon the 2007 strategy. This strategy recognizes the continuing lack of network interoperability across the federal government without clearly identifying methods to remedy these barriers to information sharing. The need for unifying government computer systems in a cloud architecture is clearly articulated. Also, recommending tagging information to enable correlating related information. This strategy provides a visionary model for long term information sharing.

The analysis of national strategies aimed to identify gaps in information sharing to combat TOC. Emerging from this analysis is recognition of the interdependence between TOC and terrorist organizations. Following the terrorist acts on 9/11, national strategy was largely focused on the immediate threat by establishing and reorganizing agencies and departments within the federal government. As the war on terror persisted, a focus on terrorist resources and information sharing across the federal government and to state and local law enforcement emerged.

Shortcomings in these strategies become apparent. First, disparate strategies addressing foreign and domestic criminal organizations disaggregates the threat. NSSs progressively address threat of TOC and the interdependence of criminal activities to resource terrorist organizations. A seam is revealed by separating these criminal organizations. Second, the absence of a directive to fuse computer networks is revealed. More recent strategies emerge which identify the need to share information and implement technologic solutions to combat terrorist and criminal threats. Although these strategies fall short of mandating the integration of computer networks across the federal

government. Finally, the absence of a lead agency to combat TOC. Such an agency would provide synchronization of effort across federal and local governments.

Organizational Level

Any approach attempting to cleanly define organizational cultures is inherently flawed. Researchers from various fields of study have widely varying and conflicting definitions and approaches to studying organizational cultures. For the purposes of this research, organizational culture is defined as "the values and behaviors that contribute to the unique social and psychological environment of an organization."[187]

For the purposes of this research, organizational boundaries are introduced. Due to time constraints, this study is limited to generalizations on organizational cultures. Although, further comparative analysis on organizational cultures across the federal government could reveal additional gaps.

Organizational cultures within the federal government emerge from numerous aspects. These aspects are derived from leadership, legal authorities, and history. These organizational cultures subsequently stove pipe information to protect organizational power. This introduction to organizational cultures examines the impacts of these boundaries on information sharing.

There are 440 agencies and departments in the U.S. federal government.[188] Each representing organizational cultures and subcultures, led by presidential appointees who

---

[187] The Business Dictionary, "Organizational Culture," accessed April 15, 2017, http://www.businessdictionary.com/definition/organizational-culture.html.

[188] National Records and Archive Administration, "Federal Register," accessed June 5, 2017, https://www.federalregister.gov/agencies.

are replaced every four to eight years. Career civil servants serve as the continuity to maintain functionality and are the cultural standard bearers. These cultures are exponentially more difficult to change due to these considerations. For this reason, bureaucratic boundaries between these organizations present challenges for effective information sharing.

In 1996, Congress initiated a study on the structure and authorities within the IC. This study titled *The Intelligence Community in the 21st Century,* attempted to address evolving threats following the fall of the Soviet Union and globalization. Over 40 senior intelligence and national security officials currently serving, their predecessors, and academics contributed to this study. Germaine to this research was the finding for the requirement to inculcate "an Intelligence Community in which all components understand that they are part of a larger coherent process aiming at a single goal: the delivery of timely intelligence to policy makers at various levels."[189] This study recognized many shortcomings plaguing the IC to date. One of which is the absence of a senior intelligence officer to manage resources and personnel across the IC.

With the creation of the DNI in 2004, the president and congress attempted to unify the IC. Failing to align authorities with resource execution is the most critical flaw in this law. Without complete resource oversight, the DNI lacks authorities requisite to drive efficiency across the IC. Additionally, as national program managers the National Security Agency (NSA), National Reconnaissance Office (NRO), and National

[189] U.S. Congress, *The Intelligence Community in the 21st Century* (Washington, DC: Government Printing Office, 1996), 6.

Geospatial-Intelligence Agency (NGA) are Department of Defense Combat Support Agencies causing further difficulties to homogenize the IC.

On the other hand, the creation of the DHS in 2002 unified twenty-two federal department and agencies. The five core missions of DHS include "preventing terrorism and enhancing security; secure and manage our borders; enforce and administer our immigration laws; safeguard and secure cyberspace; and ensure resilience to disasters."[190] This effort provides the structure to create a new organizational culture to safeguard the homeland.

Most significant to protecting U.S. citizens are the fusion centers established to combat terrorism and to mitigate the stove piping of information. At the national level, Executive Order 13354 and later codified by the Intelligence Reform and Terrorism Prevention Act of 2004 established the NCTC. The NCTC is staffed by representatives from over thirty intelligence, military, law enforcement, and homeland security personnel with access to their respective networks to facilitate information sharing to combat terrorism.[191] This interagency body provides the capability to share terrorist related information across the whole of government. Also coordinating efforts by assigning lead agencies or departments to conduct terrorist related activities.

This fusion center concept is mirrored at the state level and in major urban areas. The DHS supports fifty-three primary fusion centers and twenty-five recognized fusion centers. These centers are administered by state, local, territory and tribal law

[190] Department of Homeland Security, "Our Mission," accessed June 5, 2017, https://www.dhs.gov/our-mission.

[191] National Counter Terrorism Center, "Overview," accessed June 5, 2017, https://www.nctc.gov/overview.html.

enforcement agencies that focus on terrorism and criminal activities. Additionally, the Federal Bureau of Investigation leads 104 Joint Terrorism Task Forces focusing on counterterrorism at this same state, local, territory and tribal law enforcement level. These organizations partner to share information from the national to the local level and vice versa.

Serving at the front line to protect U.S. citizens every day, these organizations are dependent on intelligence analyst and federal law enforcement professionals. A congressional investigation released on October 3, 2012, revealed numerous shortcomings in the conduct of these DHS fusion centers.[192] This report found multiple instances of misappropriation of resources, widespread deficiencies in information sharing capabilities, and shoddy intelligence provided by DHS contractors just to name a few. This approach to information sharing is a federal government top down solution to sharing information. The need to for horizontal information sharing remains unanswered. These fusion center efforts serve as a stop gap to combat terrorism and crime, unfortunately, falling short in operationalizing information already resident at the national and local levels.

The federal government operates hundreds of unclassified and classified computer networks. These heterogeneous computer networks both control and protect information. Organizations across the federal and local government safeguard sensitive information. However, safeguarding information from interagency partners continues. This stove piping of information identified by the 9/11 Commission continues to this day.

---

[192] U.S. Congress, Senate, *Federal Support for and Involvement in State and Local Fusion Centers* (Washington, DC: Government Printing Office, 2012).

The requirement for the fusion centers mentioned above is a byproduct of the limited access to information. These representatives, both at the NCTC and fusion centers, provide information from parent organizations. This solution to information sharing fails to address the need to share information in real time across interagency boundaries.

Organizational cultures play a powerful role in protecting equities. Organizational boundaries inhibit information sharing. Stove piped networks and cultural aversion to sharing information support these boundaries. National and local level fusion centers attempt to address this shortcoming, but fail to solve the underlying gap. Sharing information should not be a decision left to these organizational gate keepers.

Individual Level

Currently, sharing information relies on human behavior. These gate keepers are influenced by organizational cultures and individual characteristics driving decisions whether or not to share information. Introduction of the Integrated Behavioral Model (IBM) is an effort to introduce the cognitive process whether to or not to share information. The most important determination whether an intelligence analyst or law enforcement officer will share sensitive information is the motivation, depicted in figure 5 below as Do I want to share? Even with the motivation, if permitted by parent organizations, individuals require knowledge on how to disseminate said information, the information must be perceived as salient. If the environment is conducive and the individual has shared information, sensitive information may be shared with outside agencies. Below is a modified version of the IBM to depict considerations to information sharing.

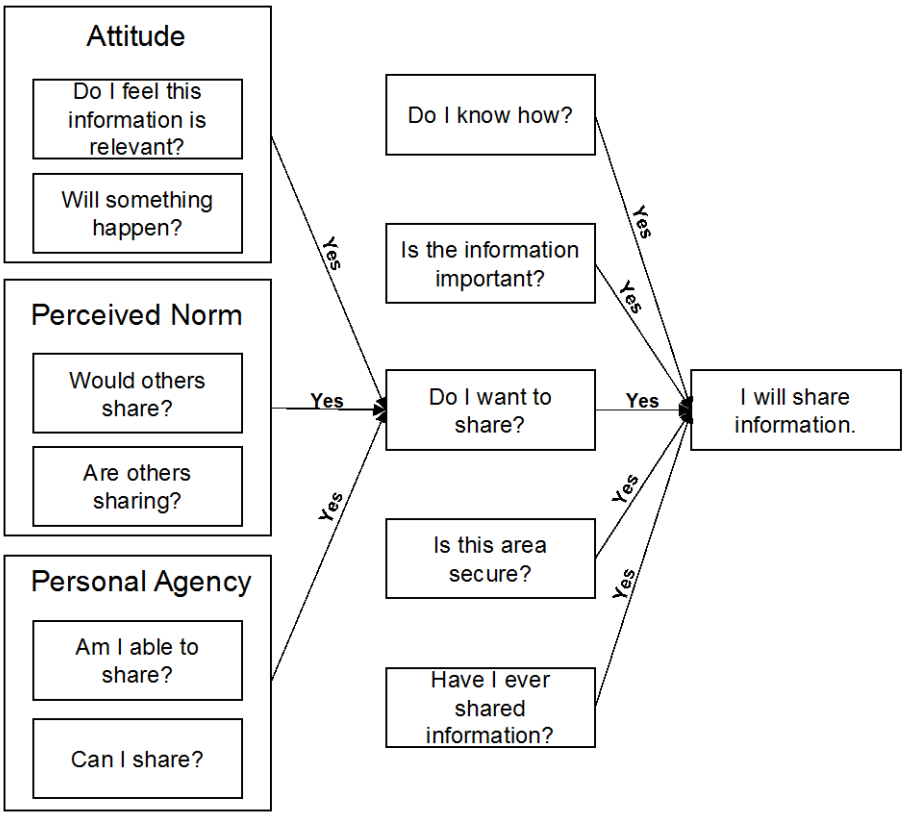

Figure 5. Information Sharing Considerations for IBM

Source: Created by author.

Relying on individuals as gate keepers to share information for combating terrorism and criminal threats has left a seam for nefarious actors to exploit. Humans are inherently flawed and unpredictable. Rather than integrating existing computer networks, the federal government deploys new networks. Examples such as the Terrorist Intensities Datamart Environment maintained by the NCTC and the Homeland Secure Data Network maintained by DHS provide terrorist related data. This approach to information sharing provides a limited solution to sharing information. Any measure short of integrating

networks to operationalize information resident across the federal government fails to address this persistent requirement.

Conclusion

Strategic level analysis reveals three shortcomings in national strategies. First, divergent strategies to combat terrorist and TOC organizations reinforces a belief that these organizations differ. The current the NSS recognizes the confluence between terrorist and TOC organizations, although, the *National Strategy to Combat Transnational Organized Crime* focuses predominately on domestic threats. Second, the absence of a directive to integrate computer networks enables organizations to stove pipe information. Although numerous national strategies identify the need to share information there is no plan to integrate federal networks. Finally, there is no lead agency to combat TOC. This lack of a lead agency causes federal agencies to embark on individual efforts to combat individual criminal activities without targeting criminal organizations.

Organizational level analysis reveals the bureaucratic boundaries to sharing information. The federal government fosters a long history of stove piping information to preserve organizational power and resourcing. In reaction to emerging threats, the U.S. Government establishes new organizations rather than addressing gaps exposed by adversaries. Establishing fusion centers fails to address the underlying gap originally identified by the 9/11 Commission to share information horizontally. These national and local fusion centers unite efforts to combat threats, but still rely on gate keepers to share information.

Individual level of analysis introduces the IBM to reveal psychological considerations employed by these gate keepers to share information. This model reveals the risks inherently assumed when relying on human behavior to share information. These intelligence analysts and law enforcement officers wield immense intellect and experience to combat terrorism and TOC. However, they lack the cability to access and share information in real time.

Chapter 5 provides the conclusions and findings of this research. Constructed to answer the secondary research questions, the primary research question will be answered. Included in chapter 5 are shortcomings identified outside the scope of this research. Finally, recommendations for further research are presented.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The purpose of this research is to answer the question: what shortcoming exists hindering information sharing across the U.S. Government to combat TOC? A structured approach based on strategic, organizational, and individual levels analysis reveal significant shortcomings. At the strategic level, three shortcomings emerged. First, national strategies to combat terrorist organizations and TOC organizations support a belief that approaches to combat these organizations diverge. In efforts to message a coherent counterterrorism and counter TOC, buzz words as whole of government and fusion attempt to provide innovative approaches. Second, national strategies recognize the need to share information to combat terrorist and TOC organizations, a directive to do so is absent. Encouraging information sharing and introducing methods to incorporate technology bring little weight when national security is at stake. Finally, there is not a lead agency to unify national efforts to combat TOC. Without an organization tasked with the responsibility to combat TOC, there can be no unity of effort.

The organizational level analysis reveals the bureaucratic boundaries inhibiting information sharing. These boundaries are in the form of stove piped computer networks and cultural adversity to information sharing. Up to this point, approaches to close this gap have relied on establishing fusion centers. These fusion centers continue to rely on gate keepers with access to stove piped information to share information. This solution brings great experience to bear, but lacks the ability to provide analysists and law enforcement a shared understanding in real time.

Individual level of analysis reveals the psychological aspects to information sharing. These gate keepers of information bring both organizational cultures and human factors presenting inherent risk. In the 21st century information sharing must not rely on human behavior. The recommendations from the 9/11 Commission to share information in real time through employing emerging technology must be implemented.

The remainder of this chapter is organized into three findings and recommendations sections. These sections correspond to the three secondary research questions. The first section will address how terrorism and TOC are two sides of the same coin. The second discusses the shortcomings in current approaches for information sharing to combat TOC. The final section discusses the potential and limitations to apply a technologic solution to information sharing.

Finding and Recommendation 1

What is the link between terrorism and TOC? Through the course of research, the linkages may be easier to understand from the stand point: how do terrorism and TOC organizationally differ? Both terrorist and TOC organizations are criminal organizations. These criminal organizations are only distinguishable by desired goals. At the middle and low levels, these organizations share financial and violent activities. The clear distinction is evident at the leadership level of these organizations. These leaders are able to autonomously oversee their organizations independent of these lower level alliances. This allows leaders to disavow their organizations' involvement, while reaping the financial benefits.

The proliferation of violence following the end of the Cold War can be correlated to the escalation of criminal activities worldwide. These criminal enterprises extract

wealth from nation states, predominantly weak or failing, stealing the ability of these states to develop institutions to care for populations. These oppressed and impoverished populations are fertile grounds for support, active or passive, for extremist groups. These extremist groups attempt to mobilize this support through narratives to create an us versus them to explain the current conditions. Meanwhile, these organizations build the capacity for violence through the extraction of resources from the very same oppressed population. The ability for extremist organizations to resource violent acts must be interdicted. This can only be achieved by combatting TOC and terrorism as a single threat.

A contemporary example of the link between TOC and terrorism can be found in Afghanistan today. Despite U.S. and international efforts to combat terrorists since 2001, Afghanistan produces 70-80 percent of the world's opium in 2017.[193] This production surged by 43 percent in 2016 despite the international efforts in Afghanistan.[194] The Islamic State of Iraq and Syria and the Taliban are both active in the opium trade. The inability to eradicate the opium trade in Afghanistan provides the financial capacity for terrorist to conduct activities worldwide.

Additionally, revenues from opium sales contribute to the instability within the government of Afghanistan.[195] The rampant corruption from this trade hinders the ability

---

[193] Anders Corr, "To Defeat Terrorism in Afghanistan, Start With Opium Crops in Nangarhar Province," *Forbes*, March 26, 2017, accessed June 5, 2017, https://www.forbes.com/sites/anderscorr/2017/03/26/to-defeat-terrorism-in-afghanistan-start-with-opium-crops-in-nangarhar-province/#1e54d6bf57d3.

[194] Ibid.

[195] Ibid.

to establish a legitimate central government. The efforts to target the production, transportation, and distribution of this terror crop lies with law enforcement.[196] It must be understood that Afghan opium farmers are not smuggling drugs into the western world. TOC syndicates provide the capability to traffic these narcotics to markets around the world. This synergistic relationship must be targeted from field to street. This inability for Afghanistan to self-govern will require external financial and military support from the United States and the international community indefinitely.

In the wake of efforts undertaken by the United States and the international community following 9/11, terrorist and criminal organizational structures became increasingly decentralized enabling lower level leadership to conduct operations autonomously. At this level, innovative and adaptive terrorists and criminals interact to advance ideological and financial goals respectively. For this reason, the United States and international partners must combat terrorism and TOC as an interwoven threat.

Recommendation

A national security strategy clearly recognizing the interdependency between terrorism and TOC should be developed to combat these threats foreign and domestic. Separate national strategies to combat terrorism and TOC should be ended. A comprehensive strategy should declare that all TOC organizations would be targeted as terrorist organizations. Additionally, these organizations must be simply identified as criminal organizations. This strategy to understand terrorist acts as a crime will provide a counter narrative to terrorist organizations' recruitment strategies.

[196] Corr.

Terrorist organizations commonly recruit based on an ideology to support violent, political goals. These ideologies can be religious, ethnic, or political. These ideological narratives can be mitigated through international understanding that these organizations are simple criminals. The current practice of surgical strikes where terrorists are killed support a martyr narrative. The author clearly recognizes that threats to national security must be eliminated. Therefore, at no point should American citizens or national security be compromised.

The criminals who commit terrorist acts should be tried in a court of law. During these proceedings evidence, photos, video or audio, can be communicated worldwide to delegitimize the accused's organization and drive a criminal counter narrative. The venue and composition of the court should be regional by peers.

Finding and Recommendation 2

How is information currently shared to combat TOC? Organizational cultures which protect information through tightly protected access persist. Though identified as a shortcoming in the 9/11 Commission's report, no forcing function is in place to seamlessly share information across the federal government or down to local law enforcement.

The tragic events perpetrated on 9/11 provided the popular support to pass legislation long called for to adapt to a post-Cold War world. The creation of DHS provides strategic vision for twenty-two formerly fragmented departments and agencies. An additional benefit of DHS is a unified organizational culture to protect the United States and partner with border countries.

The creation of the DNI attempted to unify the IC. The DNI currently lacks the authority to manage resources, functions, and efforts within these seventeen agencies. For example, the Secretary of Defense is responsible for eight of the seventeen agencies. The Secretary of Defense approves the Military Intelligence Priorities, where the DNI is responsible for the National Intelligence Priorities. These priorities are the funding mechanism from congress. This lack of authorities enables organizational cultures that compete for capability and resources leading to duplication of effort.

Creating organizations to overcome shortcomings within existing organizations seldom addresses the underlying deficiency. To this point, the PM-ISE is a haphazard effort to solve information sharing inadequacies. The PM-ISE lacks the authorities and resources to facilitate information sharing across the U.S. Government. This office's authorities are limited to countering terrorism, weapons of mass destruction, and homeland security.

Conversely, the NCTC provides a lead agency to combat terrorism. With resident experts from across the federal government, the NCTC is able to support the development of strategic policy and coordinate efforts across the government to combat terrorism. In addition, the state fusion centers serve at the tactical edge to protect the homeland. These state fusion centers are hindered by national information access and support. These detailed personnel bring both organizational cultures and psychological factors with them. These individuals function as gate keepers who control access to information. Relying on an individual to share information introduces a significant potential for failure as depicted by the IBM.

Recommendation

To address organizational shortcomings in information sharing to combat TOC. Two recommendations are proposed. First, empower the DNI with the authority to approve the request and execution of funding within the IC. Second, reorganization within the IC is required to address organizational barriers inhibiting information sharing. Finally, designating the NCTC as the lead agency to combat terrorism and TOC due to the inextricable relationship between these organizations. These solutions to current gaps in information sharing across the federal government is urgently needed.

The first recommendation grants the DNI the requisite authority over the IC to manage intelligence priorities and funding across the IC. The information already resides within the IC to combat terrorism and TOC. There are two benefits to this recommendation. The first benefit is deconstructing organizational barriers. The DNI should have the authority to restrict initiatives leading to duplicative efforts within the IC. This will force members of the IC to become interdependent. Second, funding required for intelligence activities will decrease. By granting the authority to oversee funding requests and execution, the DNI is able to force efficiency across the IC. This authority, coupled with the efficiencies gained from organizational interdependence will provide resourcing for increasing capability and capacity to conduct intelligence activities.

The next recommendation is the reorganization of the IC. This solution is needed to support national priorities and better support operational and tactical intelligence requirements. The NSA, NGA, and NRO are currently Combat Support Agencies under the Department of Defense. These organizations should be organized under the DNI. The functions of these organizations directly support national priorities and need to be

synchronized directly by the DNI. The IC must be able to provide fused national intelligence to those at the local level and the tactical edge in real time. This recommended organizational structure of the IC is depicted in figure 6 below.

Figure 6. Recommended Intelligence Community Structure

Source: Created by author.

Lastly, designating the NCTC as the lead agency to combat TOC is urgently needed. Understanding the confluence between the threats posed by terrorist and TOC organizations supports this recommendation. The NCTC will have the information and authority to unify government efforts to combat these interwoven threats. Creation of another new organization is not necessary and will create additional cultural and technological barriers attempting to address this mutually dependent threat.

Finding and Recommendation 3

What current technology exists to enable information sharing? The evolution of cloud computing in the private sector has proven to be a more efficient and economically viable solution as compared to data centers. CIOs within the federal government continue to resist capitalizing on this technology, opting to control networks at significantly higher cost with varying cybersecurity concerns. These CIOs have the ability to make these decisions due to the current funding process from congress to departments or agencies across the government. This method of resourcing restricts the ability to execute initiatives such as Cloud First.

Recommendations

Addressing the requirement to horizontally share information across the entire government executive and legislative action is required. To accelerate the provisions in the cloud first policy, the executive branch and congress should pass legislation to mandate a five-year plan for all unclassified networks in the federal government to migrate to commercial cloud providers. Additionally, OMB CIO should be designated as the executive agent for all federal IT in the federal government, granting the OMB CIO the authorities to manage the execution of all IT funding. Subsequently, CIOs of cabinet level organizations should control all IT resources for subordinates. Any organization that does not fall under one of these CIOs should be directly managed by the OMB CIO. Any waivers must be approved by the OMB CIO. This would allow for organizations to focus on services and less on infrastructure, simultaneously reducing operational cost. The migration of unclassified networks would serve as a proof of concept for classified network migration. A timeline to establish and migrate all classified networks to a

government operated cloud architecture needs to be researched. Executive agents should be named for each classification level to follow strategy mentioned above. Private industry support is essential for successful migration of these classified networks. Cybersecurity and access control must be developed to ensure information is safeguarded.

Summary

Several shortcomings hindering information sharing to combat TOC are revealed through the course of this study. This chapter provides recommendations to close these gaps. First, a single national strategy clearly identifying terrorist and TOC organizations as two sides of the same coin is urgently needed. Combatting TOC restricts the means to carry out terrorist acts. Most importantly, degrading the ability of organized crime to extract resources from less developed countries is also required. These means can provide revenue for countries to build the capacity for institutions to protect and care for populations. In the evermore global economy these terrorist and criminal organizations will exploit any seam in effort to achieve their goals.

Second, the DNI must have the authorities necessary to unify the IC. The DNI must have the ability to manage funding requests and execution across the IC. By overseeing the budgets of departments and agencies inside the IC, the DNI is able to restrict duplication of effort. Additionally, the DNI is able to unify efforts of the IC against emerging threats. The interdependence resulting from this oversight reduces funding requirements for the IC. These resources can be utilized to grow the capabilities and capacity of the IC.

Third is the urgent requirement to reorganize the IC. The NSA, NRO, and NGA should be organized directly under the authority of the DNI. These organizations are currently Combat Support Agencies under the Department of Defense. These organizations best serve the nation as peers with the Central Intelligence Agency under the DNI to form habitual interagency relationships.

Fourth is the recommendation to designate the NCTC as the lead agency to combat TOC. These expanded authorities and resources provide both focused effort against a confluent threat and a fiscally responsible solution. Attempting to solve shortcomings by establishing a new organization is a near sighted solution. Currently, national and state fusion centers rely on gatekeepers of information. All analyst and law enforcement officials assigned to the NCTC and state fusion centers must have access to all national information to combat these threats.

Finally, a five-year plan is recommended to migrate all unclassified networks to private industry cloud services. Leveraging technology to combat the nation's adversaries is vital in the 21st century. Through the leveraging of private industry cloud architecture for unclassified capability and government development of cloud technology for classified capabilities, our reliance on gatekeepers is mitigated. National and state level fusion centers must have the ability to access information from across the enterprise to combat terrorist and TOC threats. This information already resides in stove piped networks. The barriers must be broken down.

Recommendations for Further Research

Through the course of research four essential topics for subsequent research emerged. First, organizational cultures should be studied across the federal government in

an attempt to identify further measures to drive efficiencies in both function and resourcing. Recognizing that bureaucracy is required, a mixed study incorporating quantitative and qualitative analysis may provide powerful insights to deconstruct cultural boundaries. The author recommends a primary research question for further research: how do organizational cultures affect unity of effort across the federal government? Secondary research questions offered are: (1) what interdependencies exist between federal departments and agencies; (2) how does the civilian personnel system within government organizations contribute to cultural barriers; and (3) shat are the risks and rewards inherent in organizational cultures? A study of organizational cultures within the federal government have the potential to yield boundless efficiencies in both effort and resources.

Second, cloud computing poses inherent risks both in cybersecurity and insider threats. Recognition that independent networks provide physical and virtual security, access to information in a unified cloud infrastructure reveals evolutions to manage need to know. Not all users need access to all information. Research into partitioning of information inside a cloud architecture is required. The author recommends a primary research question for further study: what are the shortcomings in cloud computing? Secondary research questions suggested include: (1) how can access to information be controlled in a cloud infrastructure; (2) how can multiple commercial cloud providers be integrated securely; and (3) how can information be accessed from a cloud infrastructure when connectivity is lost or limited? Addressing reservations revealed by both scholars and practitioners during the course of this research, a study is needed to implement wide ranging migration to cloud infrastructure.

Third, the recommendation for the restructuring of the IC, which empowers the DNI, requires further research. The recommendation at the conclusion of this research recognizes the immense power residing with the DNI. This recommendation charges the DNI with control over all intelligence in the federal government. The author recommends a primary research question: what processes exist to balance control of intelligence activities within the federal government? Secondary research questions include: (1) how can congress improve oversight of intelligence activities; (2) how can intelligence activities be protected from political influences; (3) how can national and military intelligence priorities be balanced? This study is critical for restructuring the IC as recommended in this study. There cannot be an intelligence monarch.

Finally, resourcing processes within the federal government require further research. During the course of this study, numerous senior government officials and scholars cite the inefficiency in the process by which departments and agencies request and receive resources. The author recommends a primary research question: how can the current resourcing process be improved in the federal government? Secondary research questions offered include: (1) how do federal department and agencies request and receive funding; (2) how do multinational corporations manage resources; and (3) what are the risks and rewards in the current process? A study of this nature could provide insight to improving the innovation, efficiency, adaptability, and management of federal organizations.

BIBLIOGRAPHY

Books

Clark, L., and William. E. Algaier. *Surveillance Detection: The Art of Prevention: An Effective Early Warning System for Preventing Criminal and Terrorist Acts*. Bloomington: IN: AuthorHouse, 2005.

Cline, Ray S., and Yonah Alexander. *Terrorism - The Soviet Connection*. Bristol, PA: Crane, Russak and Co., 1984.

Holmes, Leslie, ed. *Terrorism, Organised Crime and Corruption: Networks and Linkages*. Cheltenham, UK: Northampton, MA.: Edward Elgar, 2007.

Kushner, Harvey W. *Terrorism in America: A Structured Approach to Understanding the Terrorist Threat*. Springfield, IL: Charles C. Thomas, 1998.

Merriam, Sharan B. *Qualitative Research and Case Study Applications in Education.* San Francisco, CA: Jossey-Bass, 1998.

Montano, Daniel E., and Danuta Kasprzyk. "Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model." In *Health Behavior and Health Education. Theory, Research, and Practice*, edited by Barbara K. Rimer, Kasisomayajula Viswanath, and Karen Glantz, 67-96. San Fransisco, CA: John Wiley and Sons, 2008.

Rittinghouse, John W., and James F. Ransome. *Cloud Computing: Implementation, Management, and Security*. Boca Raton, FL: CRC Press, 2009.

Tamaki, Taku. "Levels of Analysis of the International System." In *Encounters with World Affairs: An Introduction to International Relations,* edited by Emilian Kavalski, 85-106. Farnham: Ashgate, 2015.

Woodiwiss, Michael. "Transnational Organized Crime: The Global Reach of American Concept." In *Transnational Organized Crime: Perspectives on Global Security,* edited by Peter Gill and Adam Edwards, 50-75. New York: Routledge, Taylor and Francis Group, 2004.

Government Documents

Chief Information Officer Council. *Federal Shared Services Implementation Guide*. Washington, DC: Government Printing Office, 2013.

Defense Information Systems Agency. *Enabling the Joint Information Environment.* Washington, DC: Defense Information Systems Agency, May 5, 2014.

Department of Defense. Department of Defense Directive 5240.01, Subject: Department of Defense Intelligence Activities. Department of Defense, Washington, DC, 1988.

_____. Department of Defense Directive 5525.5, *Department of Defense Cooperation with Civilian Law Enforcement Officials*. Washington, DC: Department of Defense, 1986.

Joint Chiefs of Staff. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, November 8, 2010 (as amended through January 31, 2011).

_____. Joint Publication 2, *Joint Intelligence.* Washington, DC: Government Printing Office, 2013.

Kundra, Vivek. *Federal Cloud Computing Strategy*. Washington, DC: The White House, 2012.

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise Strategy 2016-2020*. Washington, DC: Government Printing Office, 2016.

U.S. Congress. 6 U.S. Code § 485 - Information Sharing. Washington, DC: Government Print Office, 2004.

_____. *E-Government Act of 2002*. Washington, DC: Government Print Office, 2002.

_____. *Homeland Security Act*. Washington, DC: Government Printing Office, 25 November 2002. Accessed December 19, 2012. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

_____. *Implementing Recommendations of the 9/11 Commission Act of 2007*. Washington, DC: Government Print Office, 2007.

_____. *Information Sharing Environment Annual Report to the Congress, Program Manager, Information Sharing Environment.* Washington, DC: Government Printing Office, August 2016.

_____. *Intelligence Reform and Terrorism Prevention Act of 2004*. Washington, DC: Government Print Office, 2004.

_____. Title 6 U.S. Code. Washington, DC: Government Printing Office.

_____. Title 10 U.S. Code. Washington, DC: Government Printing Office.

_____. Title 22 U.S. Code. Washington, DC: Government Printing Office.

_____. Title 50 U.S. Code. Washington, DC: Government Printing Office.

_____. *USA Patriot Act*, Public Law 107-56. Washington, DC: Government Printing Office, October 26, 2001.

U.S. Congress. Senate. *Federal Support for and Involvement in State and Local Fusion Centers.* Washington, DC: Government Print Office, 2012.

U.S. President. *National Security Strategy*. Washington, DC: The White House, 2002.

_____. *National Security Strategy.* Washington, DC: The White House, 2010.

_____. *National Security Strategy*. Washington, DC: The White House, 2015.

_____. *The President's Management Agenda.* Washington, DC: The White House, 2002.

_____. *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security.* Washington, DC: The White House, July 2011.

Undersecretary of Defense for Policy. Department of Defense Directive 3025.21, *Defense Support to Civilian Law Enforcement Agencies*. Department of Defense, Washington, DC, February 27, 2013.

_____. Department of Defense Directive 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*. Washington, DC: Department of Defense, revised August 8, 2016.

Journals/Periodicals

Ayling, Julie. "Criminal Organizations and Resilience." *International Journal of Law, Crime and Justice* 37 (2009): 182-196.

Carter, David L., and Jeremy G. Carter. "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement." *Criminal Justice and Behavior* 36, no. 12 (2009): 1323-1339.

Corr, Anders. "To Defeat Terrorism In Afghanistan, Start With Opium Crops in Nangarhar Province." *Forbes*, March 26, 2017. Accessed June 5, 2017. https://www.forbes.com/sites/anderscorr/2017/03/26/to-defeat-terrorism-in-afghanistan-start-with-opium-crops-in-nangarhar-province/#1e54d6bf57d3.

Davidson, Jacob. "Here's How Many Internet Users There Are." *Time,* May 26, 2015. Accessed January 25, 2017. http://time.com/money/3896219/internet-users-worldwide/.

Dishman, Chris. “The Leaderless Nexus: When Crime and Terror Converge.” *Studies in Conflict and Terrorism* 28 (2005): 237-252.

_____. “Terrorism, Crime, and Transformation.” *Studies in Conflict and Terrorism* 24, no. 1 (2001): 43-58.

Fountain, Jane E. “Bureaucratic reform and e-government in the United States: An Institutional Perspective.” *Routledge Handbook of Internet Politics* (2009): 99-113.

Halal, William E. “The Information Technology Revolution Computer Hardware, Software, and Services into the 21st Century.” *Technological Forecasting and Social Change* (1993): 69-86.

Mirghani, Mohamed, Michael Stankoski and Arthur Murray, “Knowledge Management and Information Technology: Can They Work in Perfect Harmony?” *Journal of Knowledge Management* 10, no. 3 (2006): 103-116.

Law, John. “Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity.” *Systems Practice and Action Research* (1992): 379-393.

Lyngaas, Sean. “ICITE Faces Cultural Resistance.” *FCW*, March 3, 2015. Accessed January 25, 2017. https://fcw.com/articles/2015/03/03/icite-faces-resistances.aspx.

Makarenko, Tamara. “The Crime–Terror Continuum: Tracing the Interplay between Transnational Organized Crime and Terrorism.” *Global Crime* 6, no. 1 (February 2004): 129-145.

Manjikian, Mary. “But My Hands Are Clean: The Ethics of Intelligence Sharing and the Problem of Complicity.” *International Journal of Intelligence and Counterintelligence* 28, no. 4 (Winter 2015-2016): 692-709.

Sanderson, Thomas M. “Transnational Terror and Organized Crime: Blurring the Lines.” *SAIS Review* 24, no. 1 (2004): 49-61.

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Action.” *Harvard National Security Journal* 3, no. 1 (2011): 85-142.

Williams, Phil, and Dimitri Vlassisi. “Combating Transnational Crime: Concepts, Activities and Responses.” *Transnational Organized Crime* 4, no. 3/4 (1998): 1-384.

Yang, Tung-mou Yang, and Yi-Jung Wu. “Exploring the Determinants of Cross-Boundary Information Sharing in the Public Sector: An E-Government Case Study in Taiwan.” *Journal of Information Science* (2014): 639-668.

Online Sources

Bannan, Karen J. “The Intelligence Community Is Sharing More Data, and Making It More Secure.” FedTech, July 22, 2016. Accessed January 25, 2017. http://www.fedtechmagazine.com/article/2016/07/intelligence-community-sharing-more-data-and-making-it-more-secure.

The Business Dictionary. “Organizational Culture.” Accessed April 15, 2017. http://www.businessdictionary.com/definition/organizational-culture.html.

Cambridge Dictionary. “Information Sharing.” Accessed June 5, 2017. http://dictionary.cambridge.org/us/dictionary/english/information-sharing.

Corbin, Kenneth. “5 Years into the ‘Cloud First Policy,’ CIOs Still Struggling.” *CIO*, April 27, 2016. Accessed January 25, 2017. http://www.cio.com/article/3061941/cloud-computing/5-years-into-the-cloud-first-policy-cios-still-struggling.html.

Department of Homeland Security. “Creation of the Department of Homeland Security.” September 24, 2015. Accessed January 25, 2017. https://www.dhs.gov/creation-department-homeland-security.

_____. “Department Six-Point Agenda,” September 23, 2013. Accessed January 25, 2017. https://www.dhs.gov/department-six-point-agenda.

_____. “Mission.” Accessed March 30, 2017. https://www.dhs.gov/mission.

_____. “Office of Intelligence and Analysis.” Accessed January 30, 2017. https://www.dhs.gov/office-intelligence-and-analysis.

Dillon, Dana R. “Breaking Down Intelligence Barriers for Homeland Security.” The Heritage Foundation, April 10, 2002. Accessed June 5, 2017. http://www.heritage.org/research/reports/2002/04/breaking-down-intelligence-barriers-for-homeland-security.

Federal Bureau of Investigation. “Transnational Organized Crime.” Accessed January 25, 2017. https://www.fbi.gov/investigate/organized-crime.

FedRAMP. “FedRAMP Overview.” General Services Administration. Accessed January 25, 2017. https://www.fedramp.gov/about-us/about/.

Konkel, Frank. “Moving to the Cloud? Change Your Culture First.” Nextgov, April 13, 2016. Accessed January 25, 2017. http://www.nextgov.com/cloud-computing/2016/04/moving-cloud-change-your-culture-first/127453/.

Merriam-Webster. “Crime.” Accessed June 5, 2017. https://www.merriam-webster.com/dictionary/crime.

_____. “Information.” Accessed June 5, 2017. https://www.merriam-webster.com/dictionary/information.

_____. “Information Technology.” Accessed June 5, 2017. https://www.merriam-webster.com/dictionary/information%20technology.

_____. “Terrorism.” Accessed June 5, 2017. https://www.merriam-webster.com/dictionary/terrorism.

National Archives and Records Administration. “Federal Register.” Accessed March 30, 2017. https://www.federalregister.gov/agencies.

Office of the Director of National Ingelligence. “How We Work.” National Counter Terrorism Center. Accessed March 30, 2017. https://www.nctc.gov/overview.html.

Oxford Dictionary. “Information Gap.” Accessed June 5, 2017. https://en.oxforddictionaries.com/definition/information_gap.

Information Sharing Environment. “The Role of PM-ISE.” Accessed January 25, 2017. https://www.ise.gov.

Statista. “E-Government Statistics and Facts.” Accessed January 25, 2017. https://www.statista.com/topics/2420/e-government/.

United Nations Office on Drugs and Crime. “Money Laundering and Globilization.” United Nations. Accessed January 25, 2017. https://www.unodc.org/unodc/en/money-laundering/globalization.html.

Wechsler, William F. “Combating Transnational Organized Crime.” Remarks Prepared for Delivery at the Washington Institute, Washington, DC, August 26, 2012. Accessed June 5, 2017. http://www.washingtoninstitute.org/html/pdf/WechslerPrepared20120426.pdf.

Papers/Reports

Armed Forces Communications and Electronics Association. *The Need to Share: The U.S. Intelligence Community and Law Enforcement*. Fairfax, VA: Armed Forces Communications and Electronics Association, April 2007.

Government Accountability Office. *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*. Washington, DC: Government Accountability Office, 2016.

Hesterman, Jennifer L. *Transnational Crime and The Criminal-Terrorist Nexus: Synergies and Corporate Trends*. Maxwell Air Force Base, AL: Air University Press. 2005.

Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing.* Gaithersburg, MD: National Institute of Standards and Technology, 2011.

Moloney-Figliola, Patricia, and Eric A. Fisher. *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*. Washington, DC: Library of Congress, 2015.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* Washington, DC: Government Printing Office, 2004.

National Infrastructure Advisory Council. *Intelligence Information Sharing, Final Report and Recommendations.* Washington, DC: National Infrastructure Advisory Council, January 10, 2012.

Perl, Raphael. "The Department of Homeland Security: Background and Challenges." In *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings, by Committee on Counterterrorism Challenges for Russia and the United States.* Washington, DC: Library of Congress, 2004.

United Nations Office on Drugs and Crime. *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes.* Vienna: United Nations, 2011. Accessed November 13, 2016. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

_____. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. Vienna: United Nations, 2010.

_____. *Transnational Organized Crime –The Global Illegal Economy.* Vienna: United Nations, 2016.

U.S. Government Accountability Office. *Joint Information Environment: DOD Needs to Strengthen Governance and Management*. Washington, DC: U.S. Government Accountability Office, July 2016.

Wagley, John R. *Transnational Organized Crime: Principal Threats and U.S. Responses.* Washington, DC: Library of Congress, 2006.